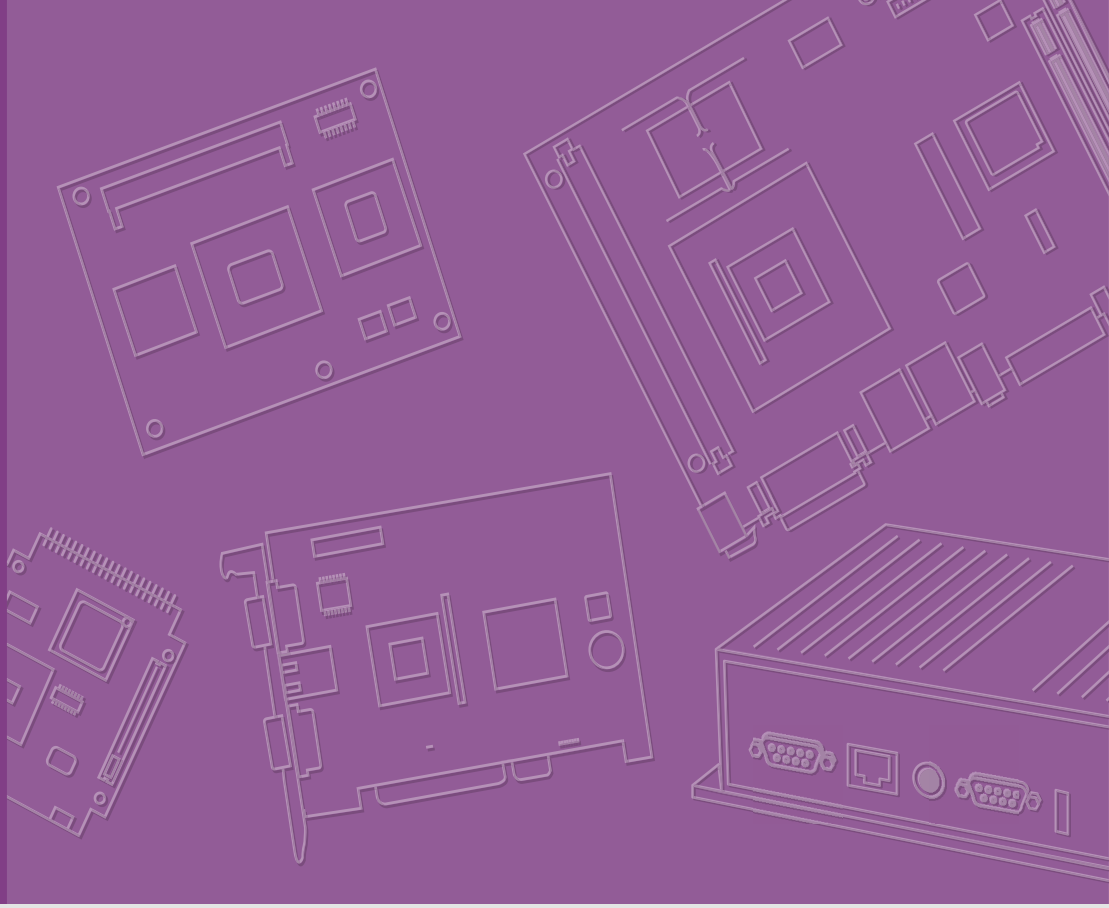


User Manual

ARK-3533

Fanless Embedded Box PC

ADVANTECH

Enabling an Intelligent Planet

Attention!

Please note:

This package contains a hard-copy user manual in Chinese for China CCC certification purposes. Please disregard the Chinese hard-copy user manual if the product is not to be sold and/or installed in China.

Copyright

The documentation and the software included with this product are copyrighted 2026 by Advantech Co., Ltd. All rights are reserved. Advantech Co., Ltd. reserves the right to make improvements in the products described in this manual at any time without notice. No part of this manual may be reproduced, copied, translated, or transmitted in any form or by any means without the prior written permission of Advantech Co., Ltd. The information provided in this manual is intended to be accurate and reliable. However, Advantech Co., Ltd. assumes no responsibility for its use, nor for any infringements of the rights of third parties that may result from its use.

Acknowledgments

Award is a trademark of Award Software International, Inc.

VIA is a trademark of VIA Technologies, Inc.

IBM, PC/AT, PS/2, and VGA are trademarks of International Business Machines Corporation.

Intel® and Pentium® are trademarks of Intel Corporation.

Microsoft Windows® is a registered trademark of Microsoft Corp.

RTL is a trademark of Realtek Semiconductor Co., Ltd.

ESS is a trademark of ESS Technology, Inc.

UMC is a trademark of United Microelectronics Corporation.

SMI is a trademark of Silicon Motion, Inc.

Creative is a trademark of Creative Technology Ltd.

Chrontel is a trademark of Chrontel Inc.

All other product names or trademarks are properties of their respective owners.

For more information about this and other Advantech products, please visit our website at:
http://www.advantech.com

For technical support and service, please visit our support website at:
http://support.advantech.com.tw/support

Part No. 2006353303 Edition 4
Printed in Taiwan June 2026

Product Warranty (2 Years)

Advantech warrants the original purchaser that each of its products will be free from defects in materials and workmanship for two years from the date of purchase.

This warranty does not apply to any products that have been repaired or altered by persons other than repair personnel authorized by Advantech, or products that have been subject to misuse, abuse, accident, or improper installation. Advantech assumes no liability under the terms of this warranty as a consequence of such events.

Because of Advantech's high quality-control standards and rigorous testing, most customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced free of charge during the warranty period. For out-of-warranty repairs, customers will be billed according to the cost of replacement materials, service time, and freight. Please consult your dealer for more details.

If you believe your product to be defective, follow the steps outlined below.

1. Collect all the information about the problem encountered. (For example, CPU speed, Advantech products used, other hardware and software used, etc.) Note anything abnormal and list any onscreen messages displayed when the problem occurs.
2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information readily available.
3. If your product is diagnosed as defective, obtain a return merchandise authorization (RMA) number from your dealer. This allows us to process your return more quickly.
4. Carefully pack the defective product, a completed Repair and Replacement Order Card, and a proof of purchase date (such as a photocopy of your sales receipt) into a shippable container. Products returned without a proof of purchase date are not eligible for warranty service.
5. Write the RMA number clearly on the outside of the package and ship the package prepaid to your dealer.

Declaration of Conformity

FCC Class B

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for assistance.

Technical Support and Assistance

1. Visit the Advantech website at www.advantech.com/support to obtain the latest product information.
2. Contact your distributor, sales representative, or Advantech's customer service center for technical support if you need additional assistance. Please have the following information ready before calling:
   - Product name and serial number
   - Description of your peripheral attachments
   - Description of your software (operating system, version, application software, etc.)
   - A complete description of the problem
   - The exact wording of any error messages

Warnings, Cautions, and Notes

Warning! *Warnings indicate conditions that could cause personal injury if not observed!*

Caution! *Cautions are included to help prevent hardware damage and data loss. For example:*

"Batteries are at risk of exploding if incorrectly installed. Do not attempt to recharge, force open, or heat the battery. Replace the battery only with the same or equivalent type as recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions."

Note! *Notes provide additional and/or optional information.*

Packing List

Before setting up the system, check that the items listed below are included and in good condition. If any item does not accord with the table, please contact your dealer immediately.

- 1 x ARK-3533 Unit
- 1 x User Manual (Simplified Chinese)
- 1 x China RoHS
- 1 x Mounting kit
- 1 x WISE-DeviceOn
- 1 x McAfee Application Control Lite / Acronis Backup 11.7 for Windows PC

Ordering Information

Part No.	CPU	DDR5	LAN	HDMI	RS-232	RS-232/ 422/485	USB 3.2	USB 2.0	M.2 B-Key	SIM	M.2 E-Key	DC Input
ARK-3533-00A1	LGA1700 Socket Type	Up to 64GB	2	2	4	4	4	4	1	1	1	9-36V DC
ARK-3533-00A1U	LGA1700 Socket Type	Up to 64GB	2	2	4	4	4	4	1	1	1	9-36V DC

Note! *CPU/Memory/Storage and operating system included by request.*

Optional Items for Default SKU

Part Number	Description
96PSA-A150W19P4-4	AC to DC adapter, DC 24V 150W, 0 ~ 40°C (-4 ~ 104°F)
96PSA-A230W24P4-4	AC to DC adapter, DC 24V 230W, -20 ~ 60°C (-4 ~ 140°F)
1702002600	Power cable 3-pin 183 cm (6 ft), USA type
1702002605	Power cable 3-pin 183 cm (6 ft), EU type
1702031801	Power cable 3-pin 183 cm (6 ft), UK type
1700000237	Power cable 3-Pin 183 cm (6 ft), PSE type

Safety Instructions

1. Read these safety instructions carefully.
2. Retain this user manual for future reference.
3. Disconnect the equipment from all power outlets before cleaning. Use only a damp cloth for cleaning. Do not use liquid or spray detergents.
4. For pluggable equipment, the power outlet socket must be located near the equipment and easily accessible.
5. Protect the equipment from humidity.
6. Place the equipment on a reliable surface during installation. Dropping or letting the equipment fall may cause damage.
7. The power outlet sockets should have grounded connections.
8. Position the power cord away from high-traffic areas. Do not place anything over the power cord.
9. All cautions and warnings on the equipment should be noted.
10. If the equipment is not used for a long time, disconnect it from the power source to avoid damage from transient overvoltage.
11. Never pour liquid into an opening. This may cause fire or electrical shock.
12. Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
13. If any of the following occurs, have the equipment checked by service personnel:
    - The power cord or plug is damaged.
    - Liquid has penetrated the equipment.
    - The equipment has been exposed to moisture.
    - The equipment is malfunctioning, or does not operate according to the user manual.
    - The equipment has been dropped and damaged.
    - The equipment shows obvious signs of breakage.
14. Do not leave the equipment in an environment with a storage temperature of below -40°C (-40°F) or above 85°C (185°F) as this may damage the components. The equipment should be kept in a controlled environment.
15. Any unverified component may cause unexpected damage. To ensure correct installation, always use the components (e.g., screws) provided in the accessory box.
16. CAUTION: The equipment is equipped with a battery-powered real-time clock circuit. There is a risk of explosion if a battery is incorrectly replaced. Replace only with the same or equivalent type as recommended by the manufacturer. Discard all used batteries according to the manufacturer's instructions.
17. Always disconnect the power cord from the chassis before manually handling the hardware. Do not implement connections or configuration changes while the device is powered on. Sudden power surges may damage sensitive electronic components.
18. In accordance with IEC 704-1:1982 specifications, the sound pressure level at the operator's position should not exceed 70 dB (A).
19. DISCLAIMER: These instructions are provided according to IEC 704-1 specifications.
    Advantech disclaims all responsibility for the accuracy of any statements contained herein.
20. Use a power cord connected to a socket-outlet with a grounded connection.
21. This product is intended to be supplied by a UL-Listed power supply suitable for use at minimum Tma 60°C (140°F) whose output meets ES1 (or SELV) and out-

put is rated: 9-36 Vdc, 25.5-6.3 A. Please contact Advantech for further information.

22. RESTRICTED ACCESS AREA: The equipment should only be installed in a Restricted Access Area.

Consignes de Sécurité

1. Veuillez lire attentivement ces instructions de sécurité.
2. Veuillez conserver ce manuel de l'utilisateur pour référence ultérieure.
3. Veuillez débrancher cet équipement de la prise secteur avant le nettoyage. Utilisez un chiffon humide. Ne pas utiliser de détergent liquide ou pulvérisé pour le nettoyage. Utilisez une feuille ou un chiffon humide pour le nettoyage.
4. Pour les équipements enfichables, la prise de courant doit être à proximité de l'équipement et doit être facilement accessible.
5. S'il vous plaît garder cet équipement de l'humidité.
6. Posez cet équipement sur une surface fiable lors de l'installation. Une chute ou une chute pourrait causer des blessures.
7. La prise de courant doit avoir une connexion mise à la terre.
8. Placez le cordon d'alimentation de sorte que personne ne puisse marcher dessus.
   Ne placez rien sur le cordon d'alimentation.
9. Tous les avertissements et mises en garde sur l'équipement doivent être notés.
10. Si l'appareil n'est pas utilisé pendant une longue période, débranchez-le du secteur pour ne pas être endommagé par une surtension transitoire.
11. Ne jamais verser de liquide dans les ouvertures de ventilation; Cela pourrait provoquer un incendie ou un choc électrique.
12. N'ouvrez jamais l'équipement. Pour des raisons de sécurité, seul le personnel de maintenance qualifié doit ouvrir l'équipement.
13. Si l'une des situations suivantes se présente, faites vérifier le matériel par le personnel de service:
    - Le cordon d'alimentation ou la fiche est endommagé.
    - Un liquide a pénétré dans l'appareil.
    - L'équipement a été exposé à l'humidité.
    - L'équipement ne fonctionne pas bien ou vous ne pouvez pas le faire. fonctionner conformément au manuel d'utilisation.
    - Equipment L'équipement est tombé et a été endommagé.
    - Equipment L'équipement présente des signes évidents de rupture.
14. Ne laissez pas cet équipement dans un environnement où la température de stockage peut être inférieure à -40°C (-40°F) ou supérieure à 85°C (185°F). Cela pourrait endommager l'équipement. L'équipement doit être dans un environnement contrôlé.
15. Tout composant non vérifié peut causer des dommages inattendus. Pour garantir une installation correcte, veuillez toujours utiliser les composants (ex. Vis) fournis avec la boîte d'accessoires.
16. ATTENTION: L'ordinateur est équipé d'un circuit d'horloge temps réel alimenté par batterie. Il y a un risque d'explosion si la batterie est remplacée de manière incorrecte. Remplacez uniquement avec le même type ou un type équivalent recommandé par le fabricant. Jetez les piles usagées conformément aux instructions du fabricant.
17. Débranchez toujours complètement le cordon d'alimentation de votre châssis lorsque vous utilisez du matériel. Ne faites pas de connexion quand l'appareil

est sous tension. Les composants électroniques sensibles peuvent être endommagés par des surtensions soudaines.

18. Niveau de pression acoustique au poste de l'opérateur selon la norme CEI 704-1: 1982 n'est pas supérieur à 70 dB (A).
19. AVERTISSEMENT: Cet ensemble d'instructions est donné conformément à la norme CEI 704-1. Advantech décline toute responsabilité quant à l'exactitude des déclarations contenues dans ce.
20. Au moyen d'un cordon d'alimentation connecté à une prise de courant avec mise à la terre.
21. Ce produit est destiné à être alimenté par un bloc d'alimentation homologué UL adapté à une utilisation à Tma 60 degrés C min. dont la sortie est conforme à ES1 (ou SELV) et dont la sortie est nominale: 9-36Vdc, 25.5-6.3A, si besoin d'aide supplémentaire, veuillez contacter Advantech pour plus d'informations.
22. ZONE D'ACCÈS RESTREINT: L'équipement ne doit être installé que dans une zone d'accès restreint.

Contents

Chapter 1 General Information 1

1.1 Introduction 2
1.2 Product Features..... 2
1.2.1 General 2
1.2.2 Display 3
1.2.3 Ethernet 3
1.3 Chipset 3
1.3.1 Functional Specifications 3
1.3.2 SUSI 4.0..... 4
1.4 Mechanical Specifications..... 5
1.4.1 Dimensions 5
Figure 1.1 ARK-3533 Mechanical Dimensions Diagram 5
1.4.2 Weight..... 5
1.5 Power Requirements..... 6
1.5.1 System Power..... 6
1.6 Operating Environment Specifications 6
1.6.1 Operating Temperature..... 6
1.6.2 Relative Humidity 6
1.6.3 Storage Temperature..... 6
1.6.4 Safety..... 6
1.6.5 EMC 6

Chapter 2 Hardware Configuration.....7

2.1 Introduction 8
2.2 Jumpers 8
2.2.1 Jumper Description 8
2.2.2 Jumper List 8
2.2.3 Jumper Locations..... 9
Figure 2.1 Jumper Layout..... 10
2.2.4 Jumper Settings 10
2.3 Connectors..... 12
2.3.1 ARK-3533 External I/O Locations 12
Figure 2.2 ARK-3533 Front and Rear I/O Connector Diagram.. 12
Figure 2.3 COM Connector..... 13
Figure 2.4 Ethernet Connector 14
Figure 2.5 Power ON/OFF Button 14
Figure 2.6 Audio Connector..... 14
Figure 2.7 LED Indicators 15
Figure 2.8 HDMI Receptacle Connector..... 15
Figure 2.9 USB 3.0 Connector..... 16
Figure 2.10DIO Connector..... 17
Figure 2.11Remote Switch Connector..... 17
Figure 2.12 Phoenix Terminal Connector 18
Figure 2.13CAN Bus Connector 18
2.4 Installation 19
2.4.1 CPU/Memory Installation 19
2.4.2 Remove the Bottom Cover..... 20
2.4.3 HDD/SSD Installation..... 21
2.4.4 M.2 Module Installation 22
2.4.5 Mounting Kit Installation..... 23
2.4.6 Wide Operating Temperature Support..... 23

Chapter 3 BIOS Settings 25

3.1 Introduction 26
3.2 Entering Setup 27
3.2.1 Main Setup..... 27
3.2.2 Advanced BIOS Features Setup..... 28
3.2.3 Chipset Configuration 73
3.2.4 Security..... 101
3.2.5 Boot 103
3.2.6 Save & Exit 104
3.2.7 NVMe RPMB Key Migration 105

Chapter 1

General Information

This chapter details background information on the ARK-3533 series.

1.1 Introduction

Advantech's ARK-3533 is an intelligent, high-performance, fanless desktop system powered by 12th/13th/14th Gen. Intel® Core™ LGA1700 and Core™ i3/i5/i7/i9 35W processors. ARK-3533 supports a maximum 35W processor and broad temperature ranges (-20 ~ 60°C / -4 ~ 140°F). It also provides multiple I/O — up to 8 x COM, 4 x GbE, 4 x USB 3.2 (2 x Gen2 + 2 x Gen1), 4 x USB 2.0, 2 x CAN Bus (optional), 1 x M.2 (B-Key), 1 x M.2 (E-Key), 1 x Line out, TPM 2.0 (optional), and 2x 2.5" SATA III hard drive bays.

Rugged Multi-Functional Design

The ARK-3533 adopts an advanced thermal design for its desktop processor solution. All models are fanless, and feature various quality features. These include wide operating temperatures (-20 ~ 60°C / -4 ~ 140°F), diverse expandability options, and structural strengthening. It supports diverse I/O interfaces — up to 4 x Intel® GbE, 4 x USB 3.2 (2 x Gen2 + 2 x Gen1), 4 x USB 2.0, 2 x CAN Bus (optional), 2 x 2.5" HDD, 1 x M.2 (B-Key), 1 x M.2 (E-Key) 4 x RS-232/422/485, and 4 x RS-232 COM ports.

Built-In Intelligent Management Tools — Advantech SUSI API and WISE-DeviceOn

The Advantech SUSI API provides a valuable suite of programmable APIs such as multi-level watchdog, hardware monitoring, and other user-friendly interfaces.

SUSI API is an intelligent self-management cross-platform tool that monitors the system's status for problems and takes action in the event of abnormalities. SUSI API offers a boot-up guarantee in critical, low-temperature environments so systems can automatically recover when voltages dip. SUSI API makes the entire system more reliable and intelligent. ARK-3533 also supports Advantech's own WISE-DeviceOn, which provides easy remote management so users can monitor, configure, and control a large number of terminals to make maintenance and system recovery simpler.

1.2 Product Features

1.2.1 General

- **CPU:** 12th/13th/14th Gen. Intel® Core™ i3/i5/i7 LGA1700 desktop processor (up to 35W)
- **System Chipset:** Intel® H610E
- **BIOS:** AMI EFI 256 Mbit
- **System Memory:** DDR5 4800Mhz up to 64GB
- **Watchdog Timer:** Single chip watchdog 255-level interval timer, set up by software
- **I/O Interface:** 4 x RS232/422/485, 4 x RS232
- **USB:** 4 x USB 3.2 (2 x Gen2 + 2 x Gen1), 4 x USB 2.0 compliant ports
- **Audio:** High Definition Audio (HD), Line-out/Mic-in
- **Storage:** 2 x 2.5" HDD drive bays (9.5 mm / 0.374 in height)
- Expansion Interface:
  - 1 x M.2 with SIM holder (B-Key for NVME, SATA, LTE/5G modules)
  - 1 x M.2 (E-Key for Wi-Fi, suggested installation at Advantech manufacturing)
  - Add-On Card Slot: AMO-R040 (by option) for 2 x PCI
- **TPM:** TPM 2.0 (Optional)

1.2.2 Display

- **Controller:** According to customer-specified CPU selection
- **Resolution:**
  - HDMI: supports HDMI 2.0, 4096 x 2160 @60Hz
- **Dual Display:**
  - HDMI + HDMI (Default)
  - DP + DP (Supported by project)
  - DP + HDMI (Supported by project)

1.2.3 Ethernet

- **Chipset:**
  - LAN1 Intel® i219-LM
  - LAN2/3/4 Intel® i226-V
- **Speed:**
  - LAN1 10/100/1000 Mbps
  - LAN2/3/4 10/100/1000/2500 Mbps

1.3 Chipset

1.3.1 Functional Specifications

1.3.1.1 Processor

Table 1.1: Processor	
Processor	Supports 12/13/14th Gen. Intel® LGA1700 processor (up to 35W)
Memory	Supports DDR5 4800 MHz up to 64GB 2 x 262-pin SODIMM socket type

1.3.1.2 Chipset

Internal Graphics Features

- DirectX 12, OpenGL 4.5
- HDMI + HDMI (DP supported by project)
- Intel® Display Power saving technology 6.0

Video Accelerator

- HW accelerated Media Decode: H.265/HEVC, H.264/MPEG-4 AVC, MPEG-2, VC-1/WMV9, JPEG/MJPEG, VP8 and VP9
- HW accelerated Media Encode: H. H.265/HEVC, H.264/MPEG-4 AVC, MPEG-2, JPEG/MJPEG and VP8

SATA Interface

- Supports several optional selections of Serial ATA III
- Supports SATA data transfer rates of up to 6 Gb/s
- Integrated AHCI controller

USB Interface

- 1 x XHCI Host Controller, supporting SuperSpeed USB 3.2 Gen1/Gen2
- 1 x EHCI Host Controllers, supporting HighSpeed USB 2.0 ports
- Supports wake-up from sleep states S3
- USB1/2 Maximum 1.5A

Power Management

- Supports ACPI
- ACPI-defined power states (processor-driven C states)
- ACPI Power Management Timer
- SMI# generation

1.3.1.3 Others

Serial Ports

- Up to 8 x serial ports
- Supports IRQ sharing among serial ports under Microsoft
- COM1, COM2, COM5, COM6: RS-232/422/485
- COM3, COM4, COM7, COM8: RS-232

Ethernet

LAN1 Intel i219LM, LAN2/3/4 Intel i226-V

- I219LM Support up to 10/100/1000 Mbps
- I226V Support up to 10/100/1000/2500Mbps
- LAN Connectors: Phone Jack RJ-45 8P 90D (F)

Audio

Audio Codec: ALC888S-VD2-GR

- Compliant with HD Audio specifications
- Supports 16/20/24-bit DAC and 16/20/24-bit ADC resolution
- Supports: Line-out, Mic-in
- Audio Connectors: 1 x headphone jack *

Battery Backup

- Battery 3V/210 mAh with 1 x WIRE

TPM 2.0

1.3.2 SUSI 4.0

- SUSI API
- Sequence control supported
- DIO 16-bit programmable DIO
- Watchdog timer multi-level WDT
- Programmable 1-255 sec/min
- Hardware monitor CPU temperature / input current / input voltage
- System information running HR / boot record
- 2 x CAN bus ports supported

1.4 Mechanical Specifications

1.4.1 Dimensions

200 x 75 x 215 mm / 7.87 x 2.95 x 8.46 in (W x H x D)

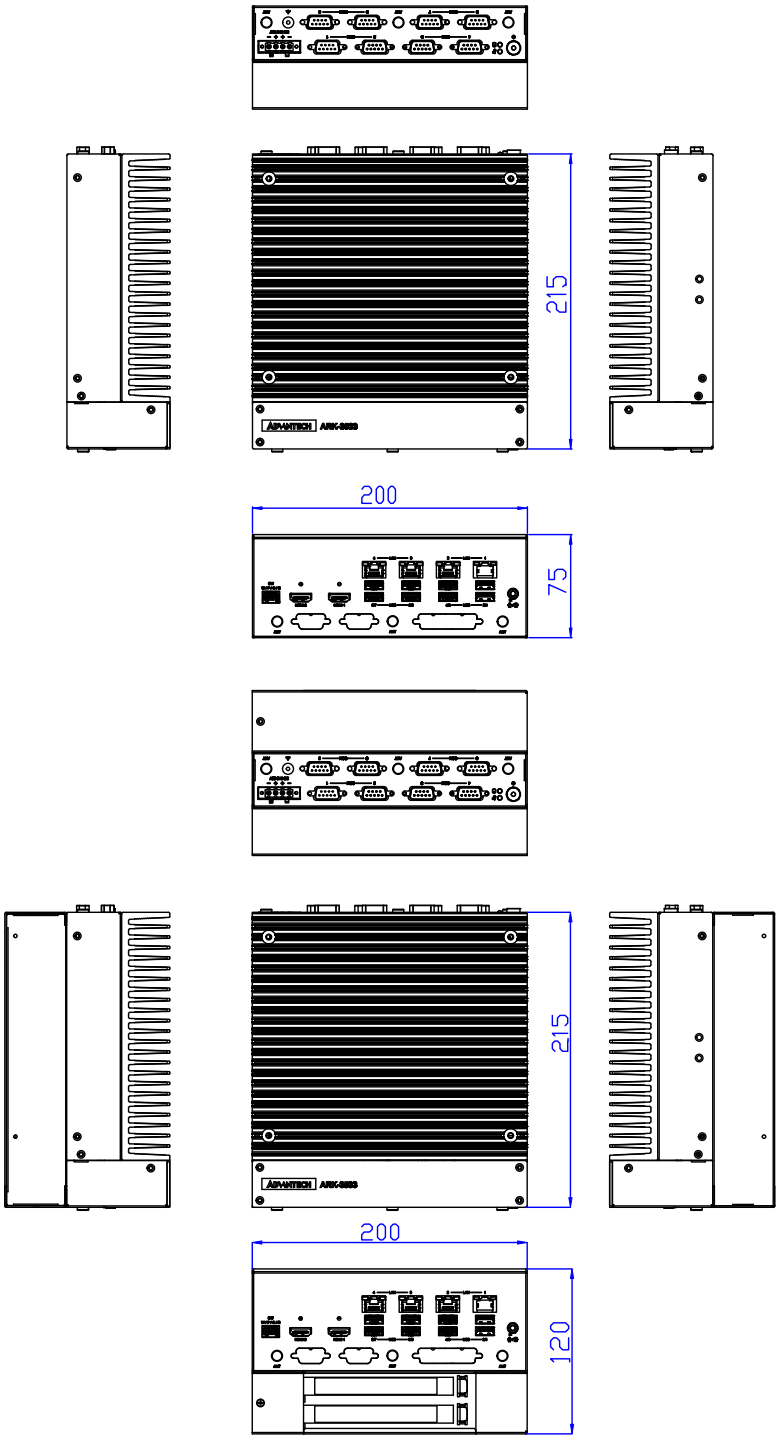


Figure 1.1 ARK-3533 Mechanical Dimensions Diagram

1.4.2 Weight

- 3.2 kg (7 lb)

1.5 Power Requirements

1.5.1 System Power

- **Minimum Power Input:** 9 ~ 36 V_{DC}
- **Optional Adapter:**
  - 150W @19V/7.89A power adapter (optional)
  - 230W @ 24V/9.58A power adapter (optional)

1.6 Operating Environment Specifications

1.6.1 Operating Temperature

- With extended peripherals: -20 ~ 60°C (-4 ~ 140°F) with 0.7 m/s airflow

1.6.2 Relative Humidity

- 95% @40°C (104°F) (non-condensing)

1.6.3 Storage Temperature

- -40 ~ 85°C (-4 ~ 185°F)

1.6.4 Safety

- UL, CB, CCC, BSMI

1.6.5 EMC

- CE/FCC Class B, CCC, BSMI

Chapter 2

Hardware Configuration

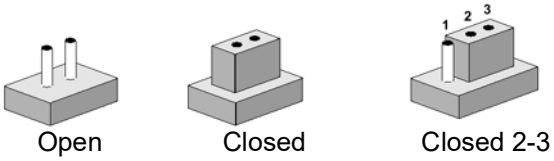
2.1 Introduction

The following sections show the internal jumper settings and the external connector pin assignments for different applications.

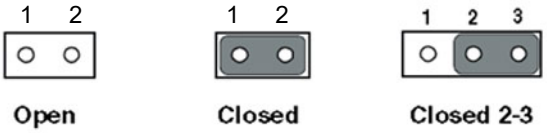
2.2 Jumpers

2.2.1 Jumper Description

You may configure ARK-3533 to match the needs of your application by setting jumpers. A jumper is a metal bridge used to close an electric circuit. It consists of two metal pins and a small metal clip (often protected by a plastic cover) that slides over the pins to connect them. To close a jumper, you connect the pins with the clip. To open a jumper, remove the clip. Sometimes a jumper will have three pins, labeled 1, 2, and 3. In this case you would connect either pins 1 and 2, or 2 and 3.



The jumper settings are schematically depicted in this manual as follows.



A pair of needle-nose pliers may be helpful when working with jumpers. If you have any doubts about the best hardware configuration for your application, contact your local distributor or sales representative before you make any changes. Generally, you simply need a standard cable to make most connections.

2.2.2 Jumper List

Table 2.1: Jumper List	
CN7	Auto Power On Setting
CLCMOS1	Clear CMOS
JSETCOM1_V1	COM1 RI power setting
CN20	M.2 B-Key Power selection
ERP1	ERP Mode setting

2.2.3 Jumper Locations

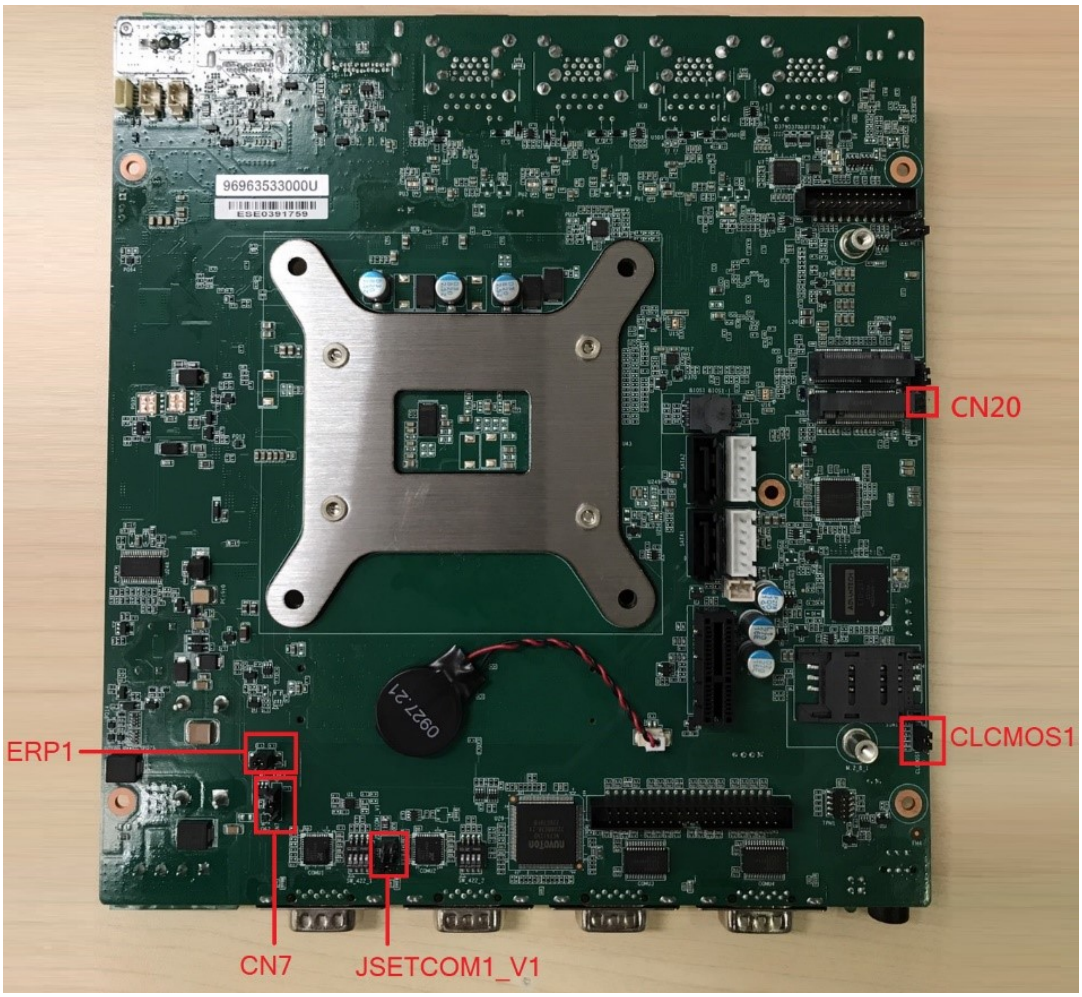
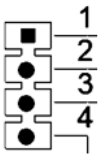


Figure 2.1 Jumper Layout

2.2.4 Jumper Settings

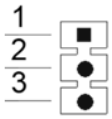
2.2.4.1 Auto Power On Setting (CN7)

Table 2.2: CN7 Auto Power On Setting	
Part Number	1653004101
Footprint	HD_4x1P_79_D
Description	PIN HEADER 4 x 1P 2.0mm 180D(M) DIP 21N12050
Setting	Function
(1-2)	Power Button for Power On (Default)
(3-4)	Auto Power On



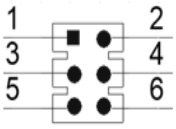
2.2.4.2 Clear CMOS Setting (CLCMOS1)

Table 2.3: CLCMOS1 Clear CMOS Setting	
Part Number	1653003101-03
Footprint	HD_3x1P_79_D
Description	PIN HEADER 3 x 1P 2.0 mm 180D(M) DIP 2000-13 WS
Setting	Function
(1-2)	Normal Operation (Default)
(2-3)	Clear CMOS



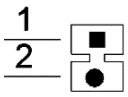
2.2.4.3 COM1 RI Power Setting (JSETCOM1_V1)

Table 2.4: JSETCOM1_V1 COM1 RI Power Setting	
Part Number	1653003201
Footprint	HD_3x2P_79_D
Description	PIN HEADER 3 x 2P 2.0 mm 180D(M) DIP 21N22050
Setting	Function
(1-2)	Normal (default)
(3-4)	+5V
(5-6)	+12V



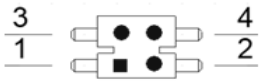
2.2.4.4 M.2 B-Key Power Setting (CN20)

Table 2.5: CN20 M.2 B-Key Power Setting	
Part Number	1653008215-01
Footprint	HD_3x2P_79_D
Description	PIN HEADER 3 x 2P 2.0 mm 180D(M) DIP 21N22050
Setting	Function
(1-2)	+3.8V power for M.2 B-Key
(NC)	+3.3V power for M.2 B-Key (default)



2.2.4.5 ERP Power Saving Mode Setting (ERP1)

Table 2.6: ERP Power Saving Mode Setting	
Part Number	1653000014
Footprint	HD_2x2P_79
Description	PIN HEADER 2 x 2P 2.00 mm 180D(M) SMD 21N22050
Setting	Function
(1-2)	Normal operation (default)
(3-4)	ERP Power saving mode



2.3 Connectors

2.3.1 ARK-3533 External I/O Locations

1. LAN 1 up to 10/100/1000 Mbps
   LAN 2 up to 10/100/1000/2500Mbps
2. USB 3.2 Gen2: USB1~2
   USB 3.2 Gen1: USB3~4
   USB 2.0: USB5~8
3. RS-232: COM3/4/7/8
   RS-232/422/485: COM1/2/5/6

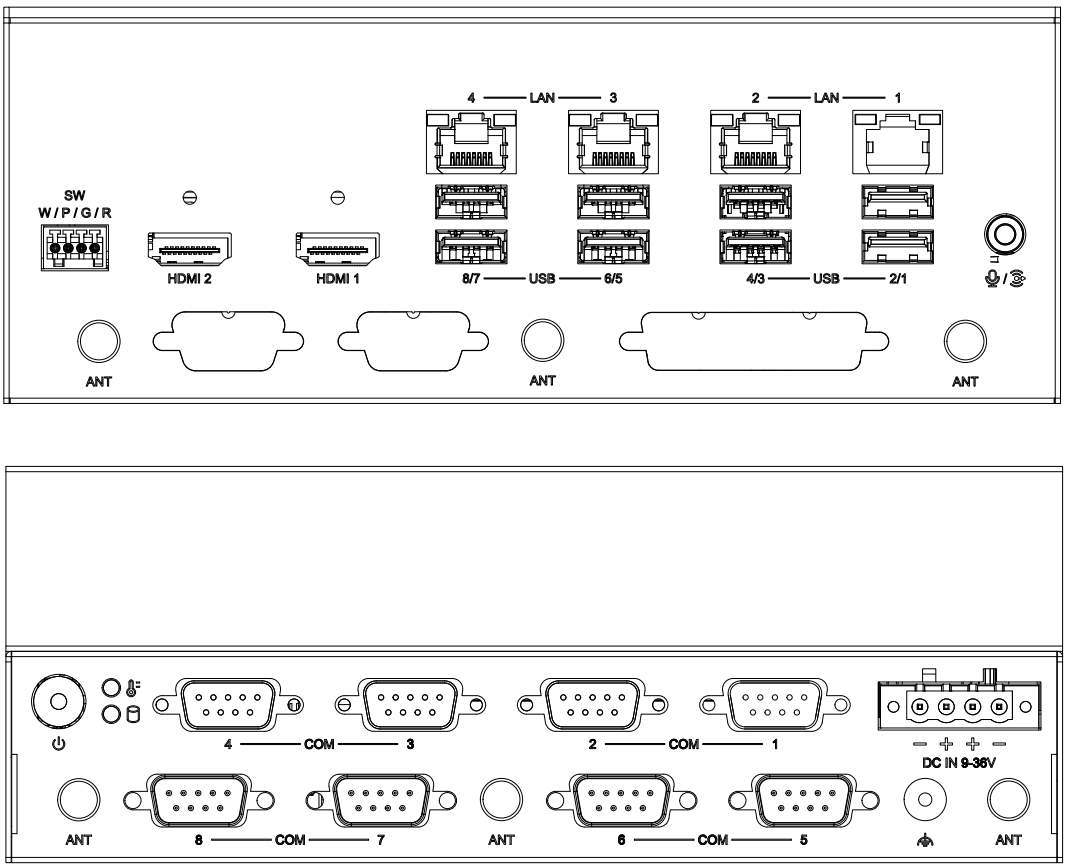


Figure 2.2 ARK-3533 Front and Rear I/O Connector Diagram

2.3.1.1 COM Connector

The ARK-3533 provides up to eight D-sub 9-pin connectors, which offer RS-232/422/485 serial communication interface ports. The default setting is RS-232, the mode RS-422/ 485 of ARK-3533 COM1/2/5/6 can be supported via the BIOS settings. COM3/4/7/8 supports RS-232.

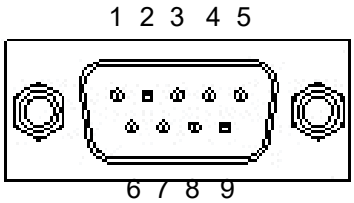


Figure 2.3 COM Connector

Table 2.7: COM Connector Pin Assignments

	RS-232	RS-422	RS-485
Pin	**Signal Name**	**Signal Name**	**Signal Name**
1	DCD	Tx-	DATA-
2	RxD	Tx+	DATA+
3	TxD	Rx+	NC
4	DTR	Rx-	NC
5	GND	GND	GND
6	DSR	NC	NC
7	RTS	NC	NC
8	CTS	NC	NC
9	RI	NC	NC

Note! *NC represents "No Connection".*

2.3.1.2 Ethernet Connector (LAN)

The ARK-3533 is equipped with up to 4 x Ethernet controllers that are fully compliant with IEEE 802.3u 10/100/1000 Mbps CSMA/CD standards. These Ethernet ports provide a standard RJ-45 jack connector with LED indicators on the front side to show Active/Link status (Green LED) and Speed status (Yellow LED).

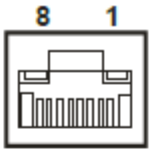


Figure 2.4 Ethernet Connector

Table 2.8: Ethernet Connector Pin Assignments

Pin	10/100/1000 BaseT Signal Name
1	TX+
2	TX-
3	RX+
4	MDI2+
5	MDI2-
6	RX-
7	MDI3+
8	MDI3-

2.3.1.3 Power On/Off Button

The ARK-3533 has a Power On/Off button with LED indicators on the front side that show “On” (Green LED) and “Off/Suspend” statuses (Orange LED). The Power but-ton sup- ports dual functions: Soft Power-On/Off (Instant off or Delay 4 Seconds then off), and Suspend.

Figure 2.5 Power ON/OFF Button

2.3.1.4 Audio Connector

The ARK-3533 features one phone jack connector that supports stereo Line-Out or Mic-In audio ports. The audio chip is controlled by ALC888S and compliant with the Azalea standards.

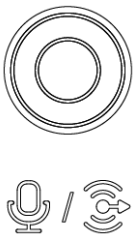


Figure 2.6 Audio Connector

2.3.1.5 LED Indicators

There are two LEDs on the front panel that indicate the system's status: the upper LED indicates thermal status (by project support only), and the lower LED indicates SATA status.

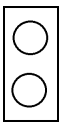


Figure 2.7 LED Indicators

2.3.1.6 HDMI Connector

An integrated, 19-pin receptacle connector HDMI Type A Interface is provided. The HDMI link supports resolutions up to 4096 x 2160 @60Hz.

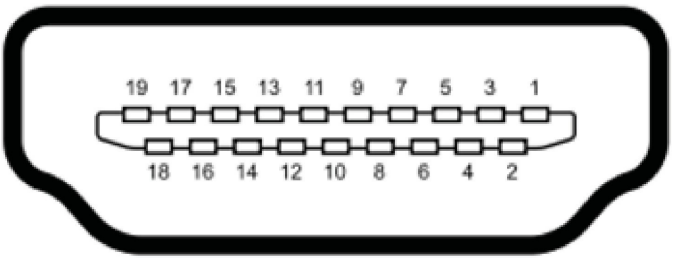


Figure 2.8 HDMI Receptacle Connector

Table 2.9: HDMI Connector Pin Assignments

Pin	Signal Name	Pin	Signal Name
1	TMDS Data 2+	2	TMDS Data 2 shield
3	TMDS Data 2-	4	TMDS Data 1+
5	TMDS Data 1 shield	6	TMDS Data 1-
7	TMDS Data 0+	8	TMDS Data 0 shield
9	TMDS Data 0-	10	TMDS clock+
11	TMDS clock shield	12	TMDS clock-
13	CEC	14	Reserved
15	SCL	16	SDA
17	DDC/CEC Ground	18	+5V
19	Hot Plug Detect		

2.3.1.7 USB 3.2 - Gen2 and Gen1

The ARK-3533 supports 2 x USB 3.2 (Gen2, 10G), 2 x USB 3.2 (Gen1, 5G). The USB interfaces comply with USB UHCI, Rev. 3.0 standards. Please refer to Table 2.10 for its pin assignments. USB 3.2 Gen1/2 connectors contain legacy pins to interface with USB 2.0 devices, and a new set of pins for USB 3.2 Gen1/2 connectivity.

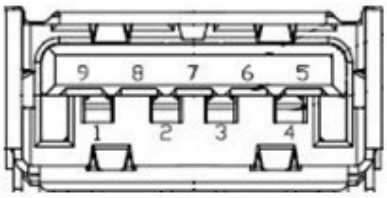


Figure 2.9 USB 3.0 Connector

Table 2.10: USB 3.2 Gen1/2 Connector Pin Assignments

Pin	Signal Name	Pin	Signal Name
1	+5V	2	USB_data-
3	USB_data+	4	GND
5	SSRX-	6	SSRX+
7	GND	8	SSTX-
9	SSTX+		

2.3.1.8 USB 2.0

The ARK-3533 (H610E) provides 4 x USB 2.0 interface connectors. The USB interface supports plug-and-play functionality.

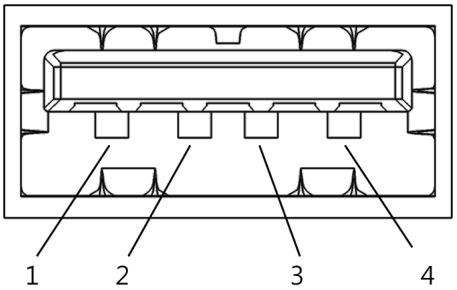


Table 2.11: USB 2.0 Pin Definition

Pin	Signal Name
1	VCC
2	USB_data
3	USB_data+
4	GND

2.3.1.9 DIO Connector (by Optional Cable)

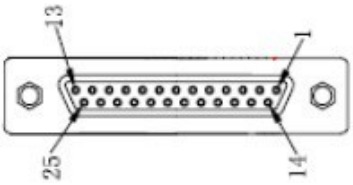


Figure 2.10 DIO Connector

Table 2.12: DIO Connector Pin Assignment

Pin	Signal Name	Pin	Signal Name
1	GND	14	GND
2	Port0 D0	15	Port1 D8
3	Port0 D1	16	Port1 D9
4	Port0 D2	17	Port1 D10
5	Port0 D3	18	Port1 D11
6	Port0 D4	19	Port1 D12
7	Port0 D5	20	Port1 D13
8	Port0 D6	21	Port1 D14
9	Port0 D7	22	Port1 D15
10	+5V	23	+5V
11	NC	24	NC
12	NC	25	NC
13	NC		

Note! *NC represents "No Connection".*

2.3.1.10 Remote Switch Connector

The ARK-3533 provides the remote switch connector for power on/off with an external cable. From the left to the right are WDT, Power Switch, GND, and Reset.

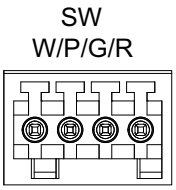


Figure 2.11 Remote Switch Connector

2.3.1.11 Phoenix Terminal Connector

The ARK-3533 supports one 4-pin Phoenix terminal power input connector. Connect the positive and negative power cables to the terminals in the power distribution connector correctly at the same time.

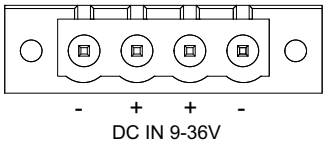


Figure 2.12 Phoenix Terminal Connector

Note!

1. *For supply connections use wires suitable for at least 105°C.*
2. *The terminal block is suitable for 14 AWG. Torque value is 7 lb-in. User copper conductors only. It must be installed by skilled person.*
3. *The terminal block uses two sets of interfaces to be installed at the same time to make it split to meet the maximum current limit, and a single pin will be limited below 16 A.*

Table 2.13: Phoenix Terminal Connector

Pin	Signal Name
-	GND
+	V-in (9-36 V)

2.3.1.12 CAN Bus (by Optional Cable)

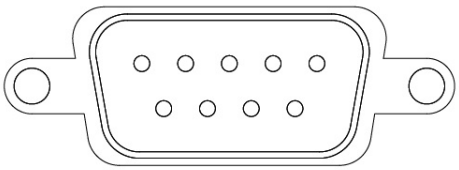


Figure 2.13 CAN Bus Connector

Table 2.14: CAN Bus Connector

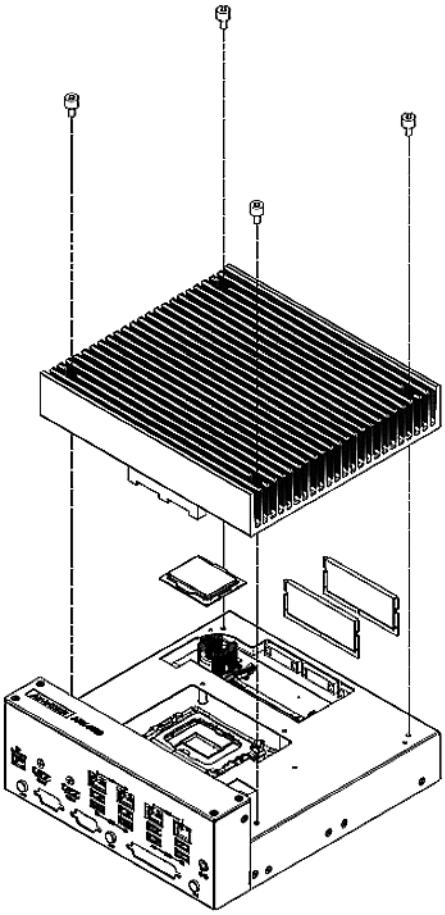
Pin	Signal Name
1	NC
2	CAN_L
3	GND
4	NC
5	NC
6	NC
7	CAN_H
8	NC
9	NC

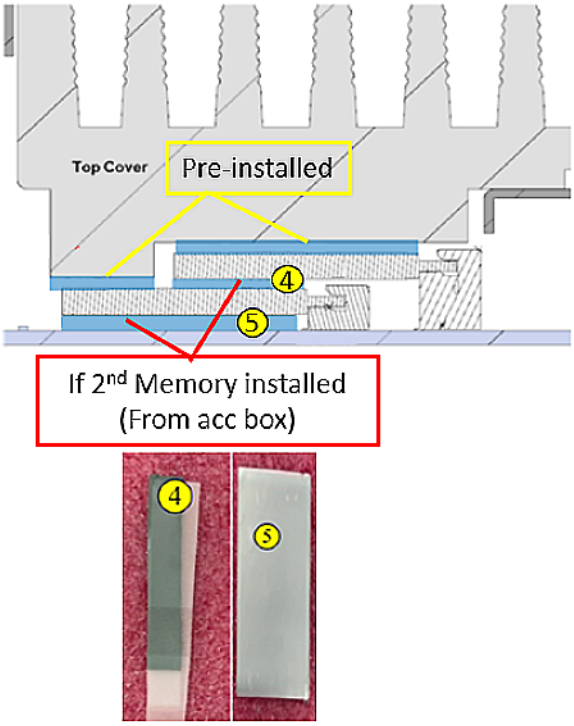
Note! *NC represents "No Connection".*

2.4 Installation

2.4.1 CPU/Memory Installation

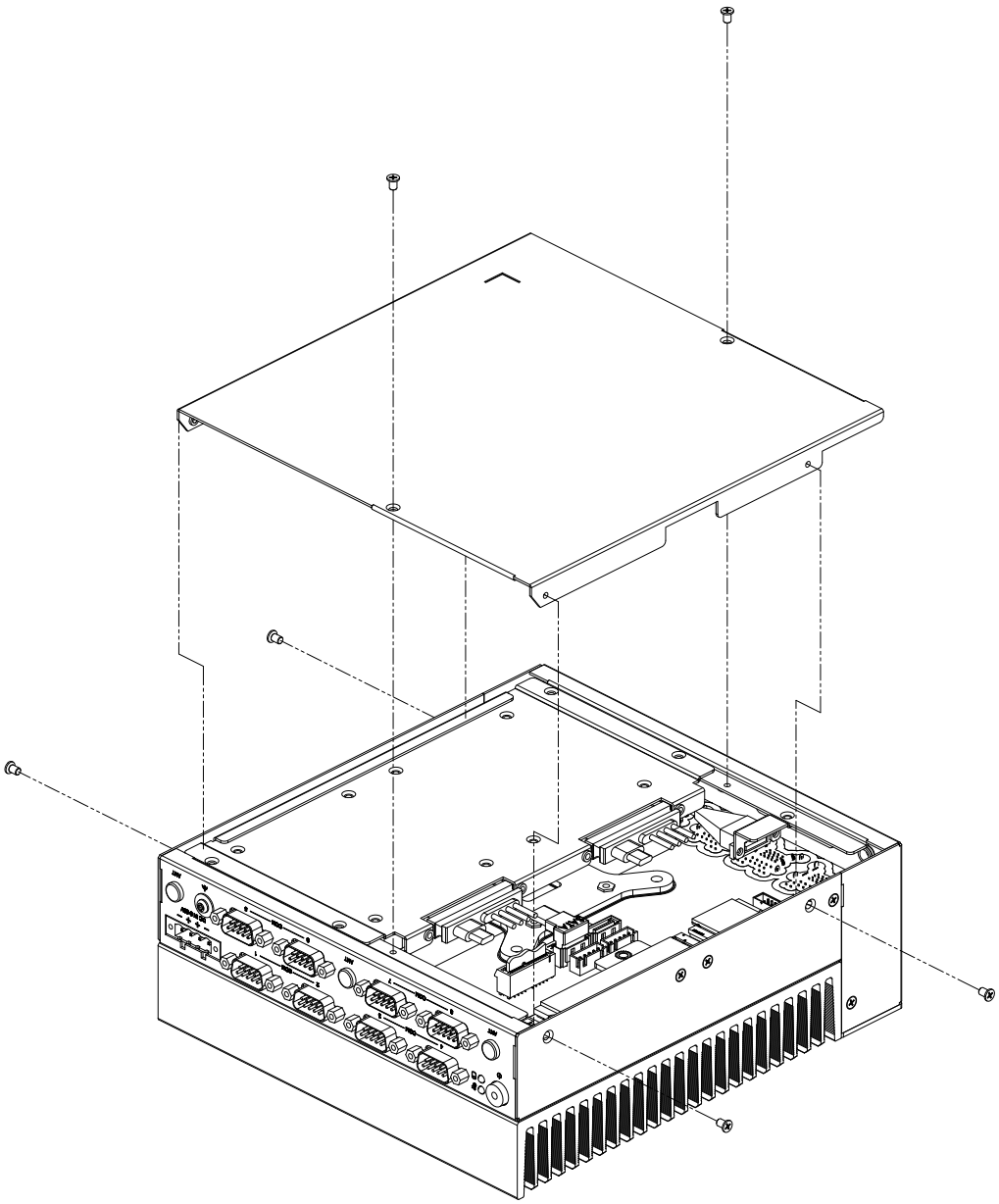
1. Unscrew the 4 screws on the top cover, and remove the top cover.
2. Install the CPU (LGA1700) and memory into the system.
3. Replace the top cover.





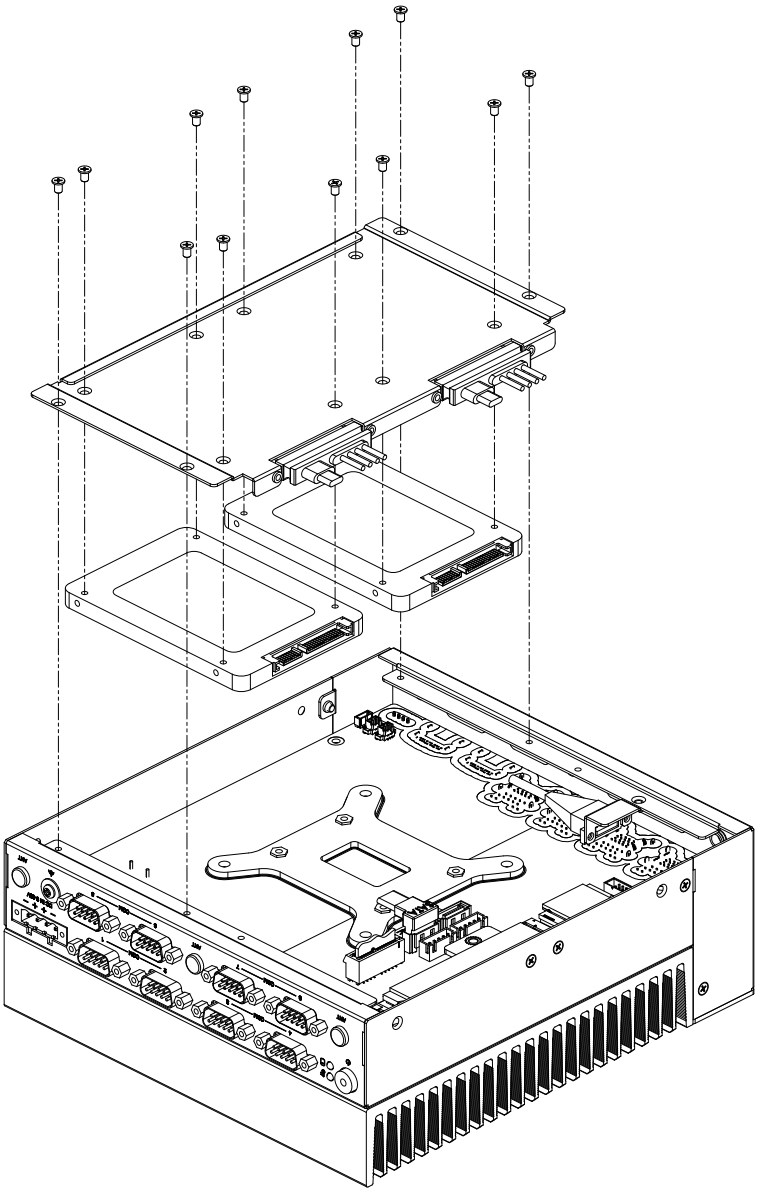
2.4.2 Remove the Bottom Cover

Unscrew the 6 screws on the bottom cover.



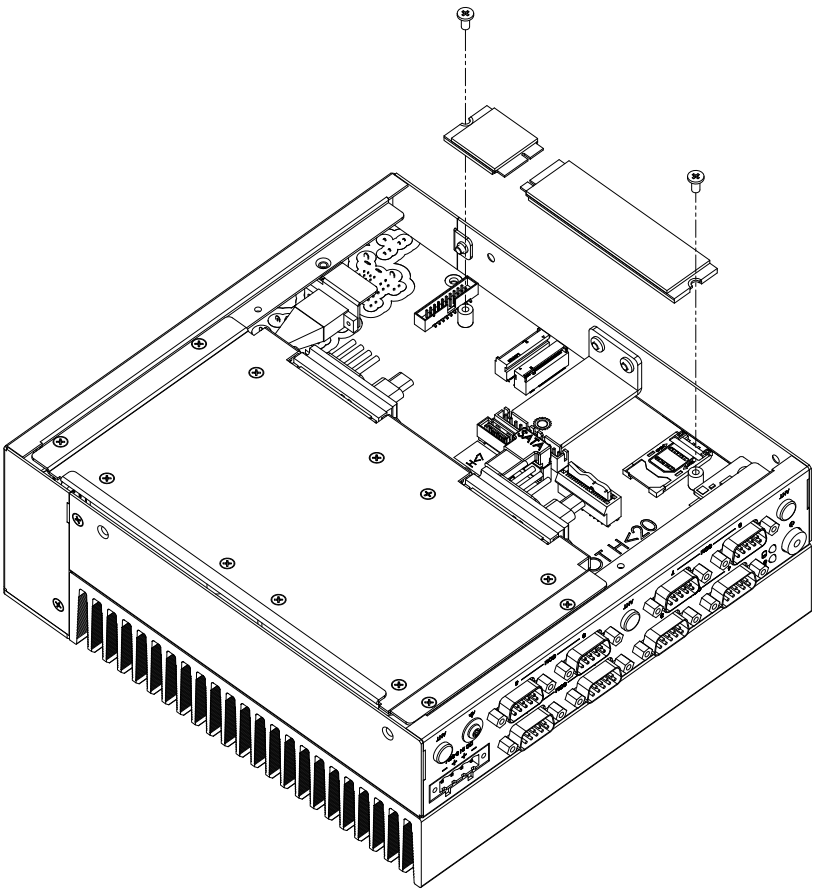
2.4.3 HDD/SSD Installation

1. Remove the bottom cover (2.4.2).
2. Remove the 4 screws for the HDD/SSD bracket.
3. Install the HDD/SSDs with 4 screws on each HDD/SSD.
4. Replace the HDD/SSD bracket and secure in place with 4 screws.
5. Replace the bottom cover and secure in place with 6 screws.



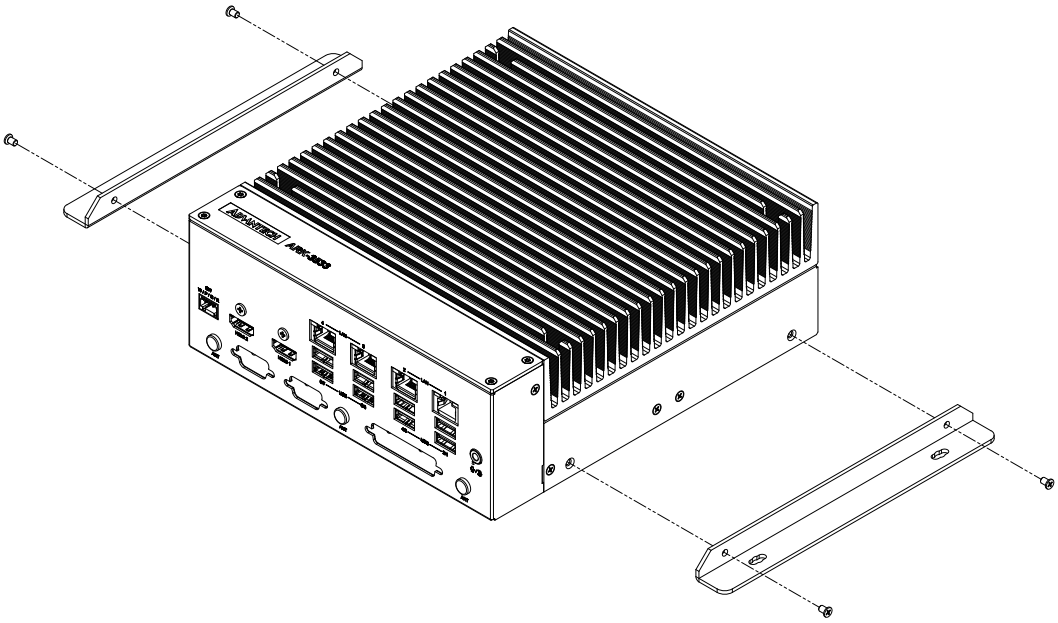
2.4.4 M.2 Module Installation

1. Remove the bottom cover (2.4.2).
2. Install the M.2 module with 1 screw (M2E).
3. Replace the bottom cover and fix it in place with 6 screws.



2.4.5 Mounting Kit Installation

1. Take out the mounting kit and 4 screws (M3x6L) from the accessory box.
   Retirez le kit de montage et les 4 vis (M3x6L) de la boîte d'accessoires.
2. Screw one of the 2 screws (M3x6L) on the left and right side and attach the system horizontally.
   Vissez chaque 2 vis (M3x6L) sur les côtés gauche et droit et fixez le système horizontalement.



2.4.6 Wide Operating Temperature Support

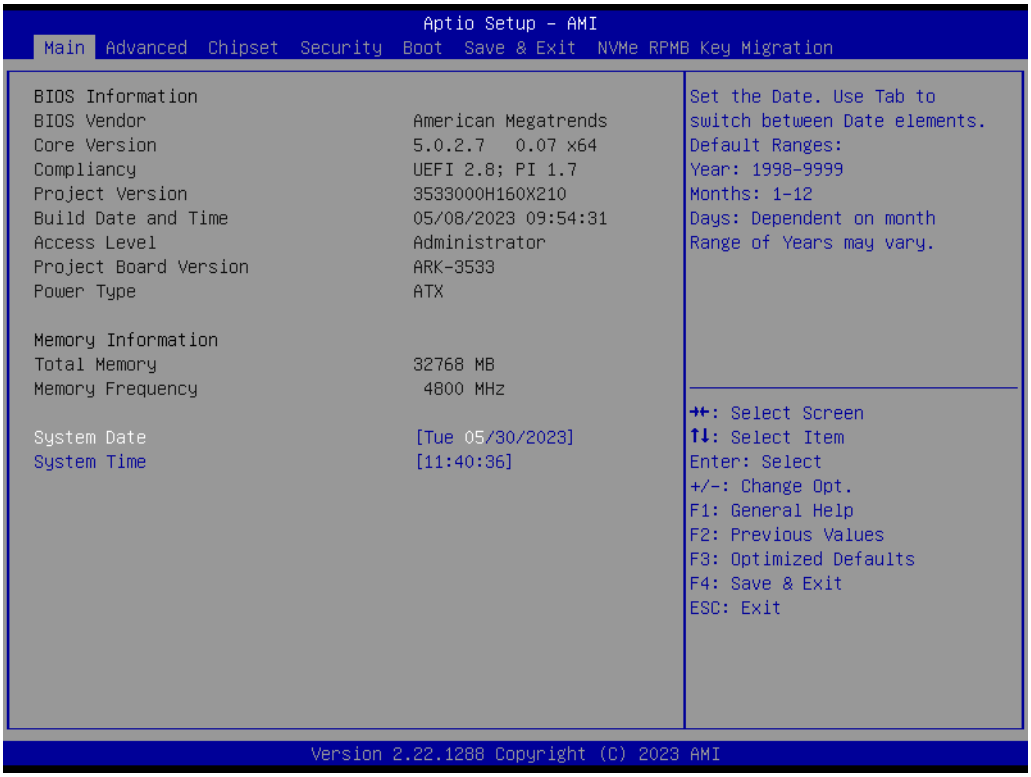
To make sure the system works well under 0°C (32°F) or over 40°C (104°F), please ensure your peripherals are I-grade. These support wide temperature operation.

Chapter 3

BIOS Settings

3.1 Introduction

AMIBIOS has been integrated into motherboards for over two decades. With the AMIBIOS Setup program, users can modify BIOS settings and control various system features. This chapter describes the basic navigation of the ARK-3533 BIOS setup screens.



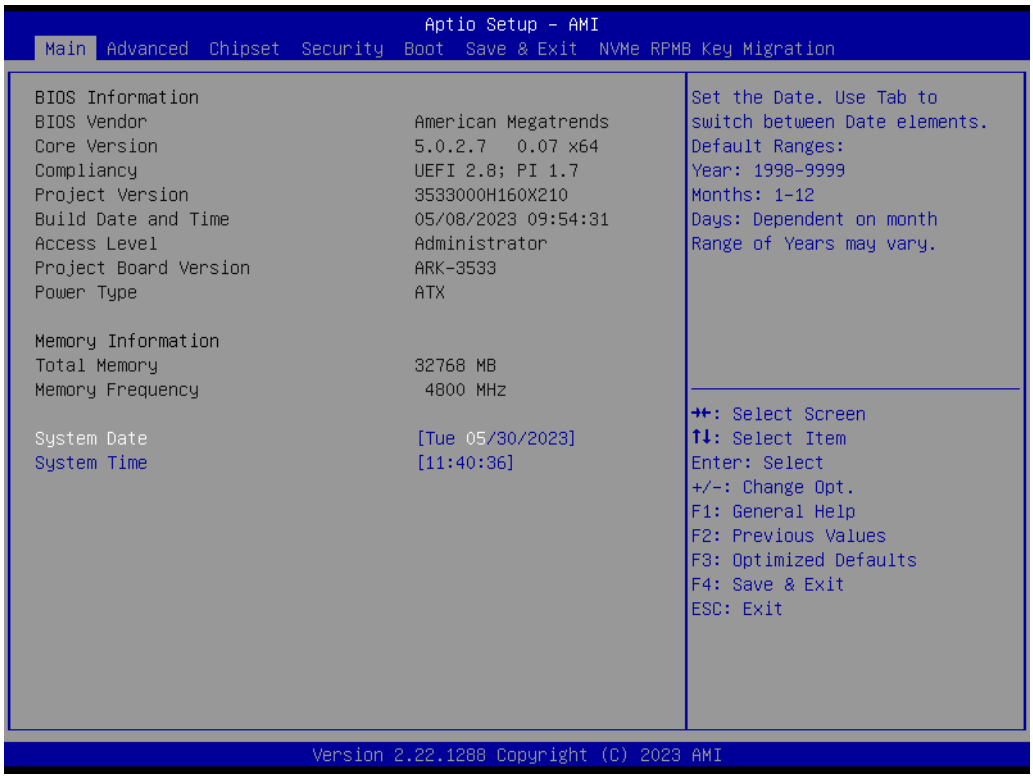
AMI's BIOS ROM has a built-in setup program that allows users to modify the basic system configuration. This information is stored in flash ROM so it retains the setup information when the power is turned off.

3.2 Entering Setup

Turn on the computer and check for the patch code. If there is a number assigned to the patch code, it means that BIOS supports your CPU. If there is no number assigned to the patch code, please contact an Advantech application engineer to obtain an up-to-date patch code file. This will ensure that your CPU's system status is valid. After ensuring that you have a number assigned to the patch code, press <DEL> and you will immediately be allowed to enter Setup.

3.2.1 Main Setup

When users first enter the BIOS Setup Utility, they will enter the Main setup screen. Users can always return to the Main setup screen by selecting the Main tab. There are two Main Setup options. They are described in this section. The Main BIOS Setup screen is shown below.



The Main BIOS setup screen has two main frames. The left frame displays all the options that can be configured. Grayed-out options cannot be configured; options in blue can. The right frame displays the key legend.

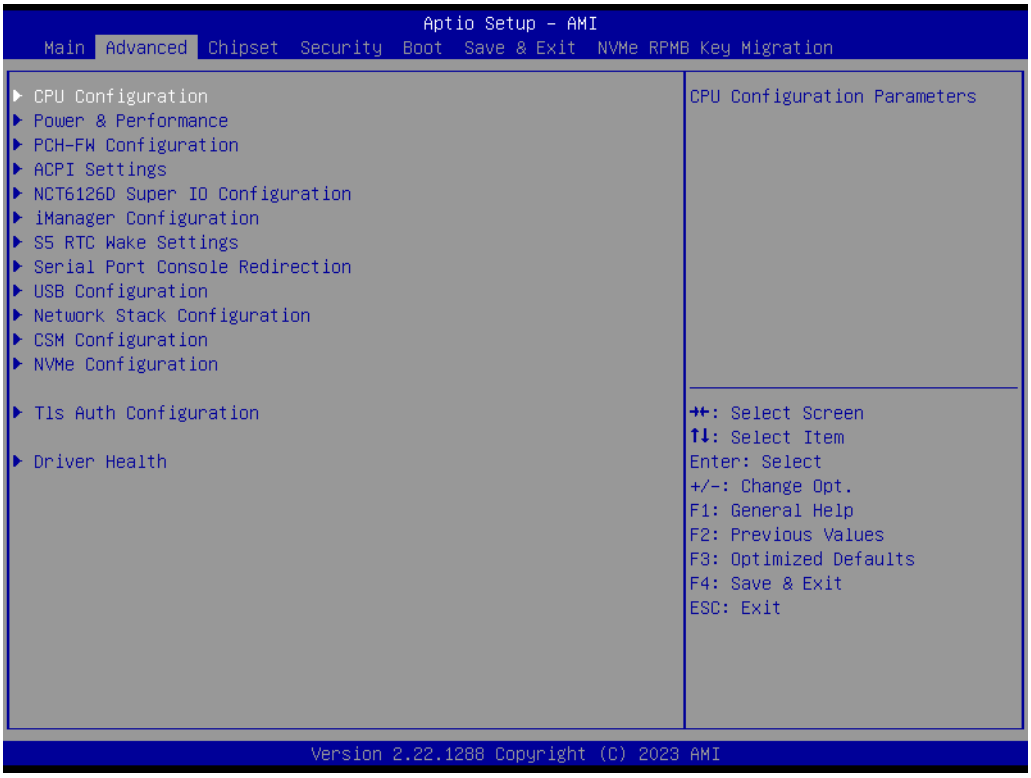
Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is highlighted in white. Often a text message will accompany it.

- **System Time / System Date**
  Use this option to change the system time and date. Highlight System Time or System Date using the <Arrow> keys. Enter new values through the keyboard. Press the <Tab> key or the <Arrow> keys to move between fields. The date must be entered in MM/DD/YY format. The time must be entered in HH:MM:SS format.

3.2.2 Advanced BIOS Features Setup

Select the Advanced tab from the ARK-3533 setup screen to enter the Advanced BIOS Setup screen. Users can select any item in the left frame of the screen, such as CPU Configuration, to go to the sub-menu for that item. Users can display an Advanced BIOS Setup option by highlighting it using the <Arrow> keys. All Advanced BIOS Setup options are described in this section. The Advanced BIOS Setup screens are shown below. The sub-menus are described on the following pages.

3.2.2.1 CPU Configuration



```
Aptio Setup - AMI
Advanced

CPU Configuration                                   Displays the P-core Information

▶ Performance-core Information

ID                                  0xB06F2
Brand String                        13th Gen Intel(R)
                                    Core(TM) i5-13500TE
Microcode Revision                  28
VMX                                 Supported
SMX/TXT                             Supported
TXT Crash Code                      0x00000000
TXT SPAD                            0x0000000000000000
Boot Guard Status                   0x00000000
Boot Guard ACM Policy Status        0x0000000000000000        →←: Select Screen
Boot Guard SACM Information         0x0000001000000000        ↑↓: Select Item
                                                              Enter: Select
C6DRAM                              [Enabled]                 +/-: Change Opt.
CPU Flex Ratio Override             [Disabled]                F1: General Help
CPU Flex Ratio Settings             13                        F2: Previous Values
Hardware Prefetcher                 [Enabled]                 F3: Optimized Defaults
Adjacent Cache Line Prefetch        [Enabled]                 F4: Save & Exit
Intel (VMX) Virtualization          [Enabled]                 ESC: Exit
Technology
PECI                                [Enabled]
AVX                                 [Enabled]

Version 2.22.1288 Copyright (C) 2023 AMI
```

```
Aptio Setup - AMI
Advanced

Boot Guard ACM Policy Status        0x0000000000000000        Enable/Disable the Avx 2
Boot Guard SACM Information         0x0000001000000000        Instructions. This is
                                                              applicable for
C6DRAM                              [Enabled]                 Performance-core only
CPU Flex Ratio Override             [Disabled]
CPU Flex Ratio Settings             13
Hardware Prefetcher                 [Enabled]
Adjacent Cache Line Prefetch        [Enabled]
Intel (VMX) Virtualization          [Enabled]
Technology
PECI                                [Enabled]
AVX                                 [Enabled]
Active Performance-cores            [All]
Active Efficient-cores              [All]                     →←: Select Screen
Hyper-Threading                     [Enabled]                 ↑↓: Select Item
BIST                                [Disabled]                Enter: Select
AP threads Idle Manner              [MWAIT Loop]              +/-: Change Opt.
AES                                 [Enabled]                 F1: General Help
MachineCheck                        [Enabled]                 F2: Previous Values
MonitorMWait                        [Enabled]                 F3: Optimized Defaults
Intel Trusted Execution Technology  [Disabled]                F4: Save & Exit
Alias Check Request                 [Disabled]                ESC: Exit
DPR Memory Size (MB)                4
Reset AUX Content                   [no]
▶ CPU SMM Enhancement

Version 2.22.1288 Copyright (C) 2023 AMI
```

- **Performance-core Information**
  Displays the P-core Information.
- **C6DRAM**
  Enable/Disable moving of DRAM contents to PRM memory when the CPU is in C6 state.

- **CPU Flex Ratio Override**
  Enable/Disable CPU Flex Ratio Programming.
- **CPU Flex Ratio Settings**
  This value must be between the Max Efficiency Ratio (LFM) and the Maximum non-turbo ratio set by hardware (HFM).
- **Hardware Prefetcher**
  To turn on/off the MLC streamer prefetcher.
- **Adjacent Cache Line Prefetch**
  To turn on/off prefetching of adjacent cache lines.
- **Intel (VMX) Virtualization Technology**
  When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
- **PECI**
  Enable/Disable PECI.
- **AVX**
  Enable/Disable the Avx 2 Instructions. This is applicable for Performance-core only.
- **Active Performance-Cores**
  Number of cores to enable in each processor package.
- **Active Efficient-cores**
  Enable/Disable Per Core Disable. When Per Core Disable Configuration is enabled, selection of Active Cores and Active Efficient-cores will be disabled.
- **Hyper-Threading**
  Enable or Disable Hyper-Threading Technology.
- **BIST**
  Enable/Disable BIST (Built-in Self Test) on reset.
- **AP threads Idle Manner**
  AP threads Idle Manner for waiting signal to run.
- **AES**
  Enable/Disable AES. (Advanced Encryption Standard)
- **MachineCheck**
  Enable/Disable Machine Check.
- **MonitorMWait**
  Enable/Disable MonitorMWait. If Disabled, the AP threads Idle Manner should not be set to MWAIT Loop.
- **Intel Trusted Execution Technology**
  Enables utilization of additional hardware capabilities provided by Intel® Trusted Execution Technology.
- **Alias Check Request**
  Enables Txt Alias Checking capability.
- **DPR memory size (MB)**
  Reserve DPR memory size (0-255) MB.
- **Reset AUX Content**
  Reset TPM Aux content. Txt may not functional after AUX content gets reset.
- **Total Memory Encryption**
  Configure Total Memory Encryption (TME) to protect DRAM data from physical attacks.
- **Legacy Game Compatibility Mode**
  When enabled, pressing the scroll lock key will toggle the Efficient-cores between being parked when Scroll Lock LED is on and un-parked when the LED is off.

```
Aptio Setup - AMI
Advanced

C6DRAM                                  [Enabled]
CPU Flex Ratio Override                 [Disabled]
CPU Flex Ratio Settings                 13
Hardware Prefetcher                     [Enabled]
Adjacent Cache Line Prefetch            [Enabled]
Intel (VMX) Virtualization              [Enabled]
Technology
PECI                                    [Enabled]
AVX                                     [Enabled]
Active Performance-cores                [All]
Active Efficient-cores                  [All]
Hyper-Threading                         [Enabled]
BIST                                    [Disabled]
AP threads Idle Manner                  [MWAIT Loop]
AES                                     [Enabled]
MachineCheck                            [Enabled]
MonitorMWait                            [Enabled]
Intel Trusted Execution Technology      [Disabled]
Alias Check Request                     [Disabled]
DPR Memory Size (MB)                    4
Reset AUX Content                       [no]
▶ CPU SMM Enhancement
Total Memory Encryption                 [Disabled]
Legacy Game Compatibility Mode          [Disabled]

CPU SMM Enhancement

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

```
Aptio Setup - AMI
Advanced

CPU SMM Enhancement

SMM Use Delay Indication                [Enabled]
SMM Use Block Indication                [Enabled]
SMM Use SMM en-US Indication            [Enabled]

Enable/Disable usage of
SMM_DELAYED MSR for MP sync in
SMI

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

- **SMM Use Delay Indication**
  Enable/Disable usage of SMM_DELAYED MSR for MP sync in SMI.
- **SMM Use Block Indication**
  Enable/Disable usage of SMM_BLOCKED MSR for MP sync in SMI.
- **SMM Use en-US Indication**
  Enable/Disable usage of SMM_ENABLE MSR for MP sync in SMI.

3.2.2.2 Power and Performance – CPU Power Management Control

```
Aptio Setup - AMI
Main  Advanced  Chipset  Security  Boot  Save & Exit  NVMe RPMB Key Migration

▶ CPU Configuration                    Power & Performance Options
▶ Power & Performance
▶ PCH-FW Configuration
▶ ACPI Settings
▶ NCT6126D Super IO Configuration
▶ iManager Configuration
▶ S5 RTC Wake Settings
▶ Serial Port Console Redirection
▶ USB Configuration
▶ Network Stack Configuration
▶ CSM Configuration
▶ NVMe Configuration
▶ Tls Auth Configuration               →←: Select Screen
▶ Driver Health                        ↑↓: Select Item
                                       Enter: Select
                                       +/-: Change Opt.
                                       F1: General Help
                                       F2: Previous Values
                                       F3: Optimized Defaults
                                       F4: Save & Exit
                                       ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

```
Aptio Setup - AMI
Advanced

Power & Performance                    CPU - Power Management Control
                                       Options
▶ CPU - Power Management Control
▶ GT - Power Management Control
                                       →←: Select Screen
                                       ↑↓: Select Item
                                       Enter: Select
                                       +/-: Change Opt.
                                       F1: General Help
                                       F2: Previous Values
                                       F3: Optimized Defaults
                                       F4: Save & Exit
                                       ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

```
Aptio Setup - AMI
Advanced

CPU - Power Management Control                    Select the performance state
                                                  that the BIOS will set
Boot performance mode              [Turbo Performance]  starting from reset vector.
Intel(R) SpeedStep(tm)             [Enabled]
Race To Halt (RTH)                 [Enabled]
Intel(R) Speed Shift Technology    [Enabled]
Per Core P State OS control mode   [Enabled]
HwP Autonomous Per Core P State    [Enabled]
HwP Autonomous EPP Grouping        [Enabled]
EPB override over PECI             [Disabled]
HwP Lock                           [Enabled]
HDC Control                        [Enabled]
  Turbo Mode                       [Enabled]
▶ View/Configure Turbo Options                    →←: Select Screen
▶ CPU VR Settings                                 ↑↓: Select Item
Platform PL1 Enable                [Enabled]      Enter: Select
Platform PL1 Power                 27000          +/-: Change Opt.
Platform PL1 Time Window           [0]            F1: General Help
Platform PL2 Enable                [Enabled]      F2: Previous Values
Platform PL2 Power                 45000          F3: Optimized Defaults
ATX Telemetry Unit                 [Watts]        F4: Save & Exit
Power Limit 4 Override             [Enabled]      ESC: Exit
Power Limit 4                      60000
Power Limit 4 Lock                 [Disabled]
C states                           [Disabled]

Version 2.22.1288 Copyright (C) 2023 AMI
```

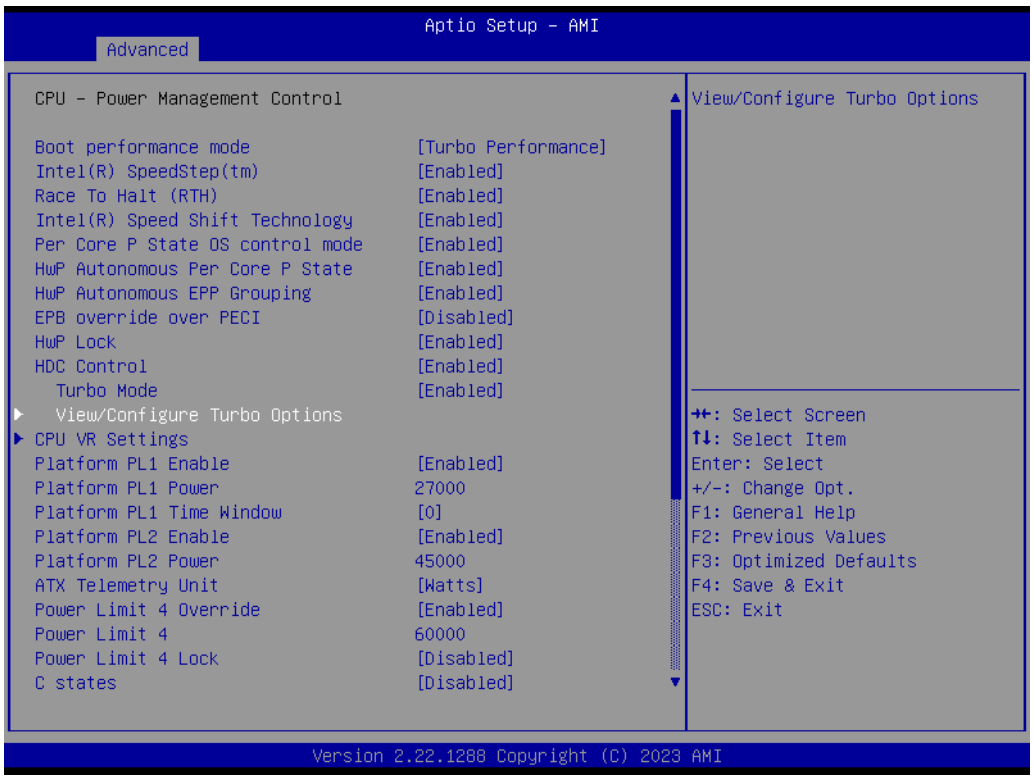
```
Aptio Setup - AMI
Advanced

HDC Control                        [Enabled]      Enable/Disable CPU Power
  Turbo Mode                       [Enabled]      Management. Allows CPU to go
▶ View/Configure Turbo Options                    to C states when it's not 100%
▶ CPU VR Settings                                 utilized.
Platform PL1 Enable                [Enabled]
Platform PL1 Power                 27000
Platform PL1 Time Window           [0]
Platform PL2 Enable                [Enabled]
Platform PL2 Power                 45000
ATX Telemetry Unit                 [Watts]
Power Limit 4 Override             [Enabled]
Power Limit 4                      60000
Power Limit 4 Lock                 [Disabled]
C states                           [Disabled]     →←: Select Screen
Thermal Monitor                    [Enabled]      ↑↓: Select Item
Interrupt Redirection Mode         [Fixed Priority]  Enter: Select
Selection                                         +/-: Change Opt.
Timed MWAIT                        [Disabled]     F1: General Help
▶ Custom P-state Table                            F2: Previous Values
Energy Performance Gain            [Disabled]     F3: Optimized Defaults
EPG DIMM Idd3N                     26             F4: Save & Exit
EPG DIMM Idd3P                     11             ESC: Exit
▶ Power Limit 3 Settings
▶ CPU Lock Configuration
Dual Tau Boost                     [Disabled]

Version 2.22.1288 Copyright (C) 2023 AMI
```

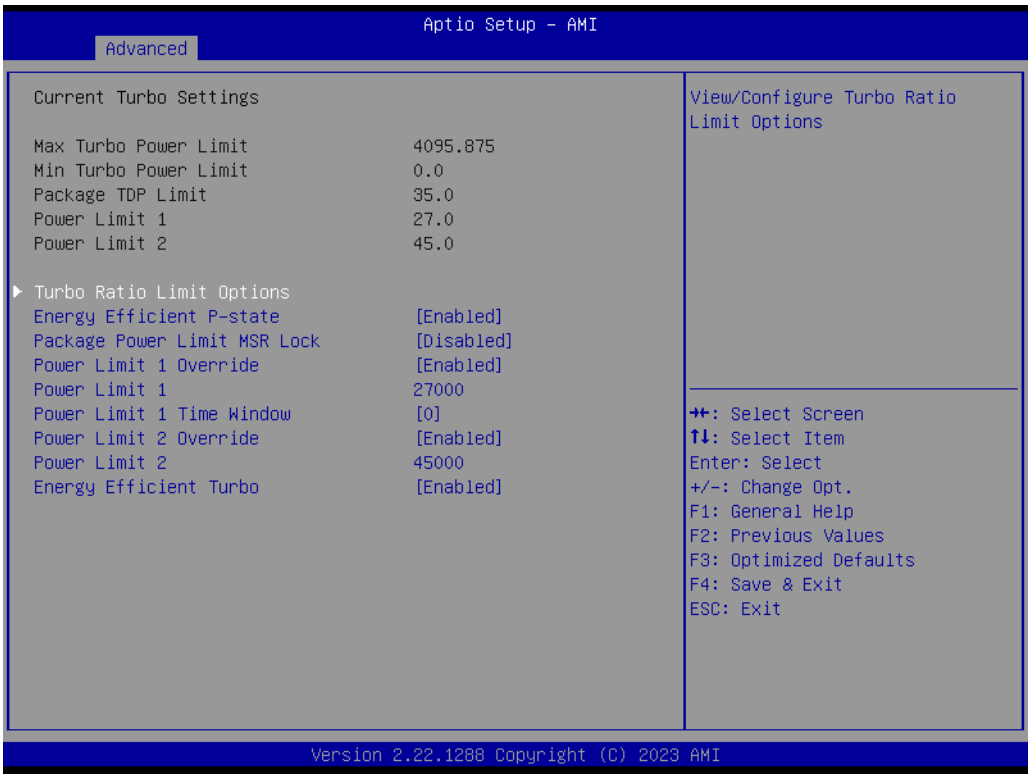
- **Boot Performance**
  Select the performance state that the BIOS will set before OS hand-off.
- **Intel® Speedstep™**
  Allows more than two frequency ranges to be supported.
- **Race to Halt (RTH)**
  Enable/Disable Race To Halt feature. RTH will dynamically increase CPU fre-

quency in order to enter pkg C-State faster to reduce overall power. (RTH is controlled through MSR 1FC bit 20)

- **Intel® Speed Shift Technology**
  Enable/Disable Intel® Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states.
- **Per core P state OS control mode**
  Enable/Disable Per Core P state OS control mode. Disabling will set Bit 31 = 1 command 0x06. When set, the highest core request is used for all other core requests.
- **Hwp Autonomous Per core P state**
  Disable Autonomous PCPS (Bit 30 = 1, command 0x11) Autonomous will request the same value for all cores all the time. Enable PCPS (default Bit 30 = 0, command 0x11)
- **Hwp Autonomous EPP grouping**
  Enable EPP grouping (default Bit 29 =0, command 0x11) Autonomous will request the same values for all cores with the same EPP. Disable EPP grouping (Bit 29 =1, command 0x11) autonomous will not necessarily request the same values for all cores with the same EPP.
- **EPB override over PECI**
  Enable/Disable EPB override over PECI. Enable by sending pcode command 0x2b, subcommand 0x3 to 1. This will allow OOB EPB PECI override control.
- **HWP Lock**
  Enable/Disable HWP Lock support in Misc Power Management MSR.
- **HDC Control**
  This option allows HDC configuration.
- **Turbo Mode**
  Enable/Disable processor Turbo Mode (requires Intel Speed Step or Intel Speed Shift to be available and enabled).
- **Platform PL1 Enable**
  Enable/Disable Platform Power Limit 1 programming.
- **Platform PL1 Power**
  Platform Power Limit 1 Power in Milli Watts.
- **Platform PL1 Time Window**
  Platform Power Limit 1 Time Window value in seconds.
- **Platform PL2 Enable**
  Enable/Disable Platform Power Limit 2 programming.
- **Platform PL2 Power**
  Platform Power Limit 2 Power in milliwatts.
- **Power Limit 4 Override**
  Enable/Disable Power Limit 4 override.
- **Power Limit 4**
  Power Limit 4 in milliwatts.
- **Power Limit 4 Lock**
  Power Limit 4 MSR 601h Lock. When enabled PL4 configurations are locked during OS. When disabled PL4 configuration can be changed during OS.
- **C states**
  Enable/Disable CPU Power Management.
- **Thermal Monitor**
  Enable/Disable Thermal Monitor.
- **Interrupt Redirection Mode Selection**
  Interrupt Redirection Mode Select for Logical Interrupts.

- **Timed MWAIT**
  Enable/Disable Timed MWAIT Support.
- **Energy Performance Gain**
  Enable/disable Energy Performance Gain.





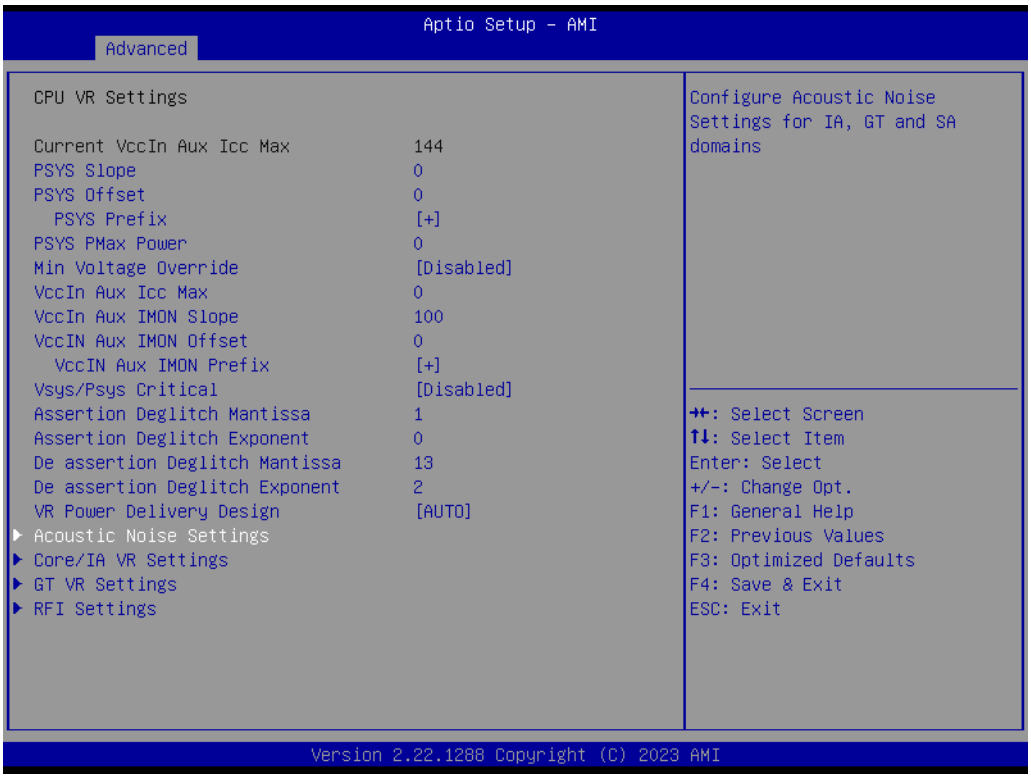
- **Energy Efficient P-state**
  Enable/Disable Energy Efficient P-state feature.
- **Package Power Limit MSR Lock**
  Enable/Disable locking of Package Power Limit settings.
- **Power Limit 1 Override**
  Enable/Disable Power Limit 1 override.
- **Power Limit 1**
  Power Limit 1 in milliwatts.
- **Power Limit 1 Time Window**
  Power Limit 1 Time Window value in seconds.
- **Power Limit 2 Override**
  Enable/Disable Power Limit 2 override.
- **Power Limit 2**
  Power Limit 2 value in milliwatts.
- **Energy Efficient Turbo**
  Enable/Disable Energy Efficient Turbo Feature. This feature will opportunistically lower the turbo frequency to increase efficiency.

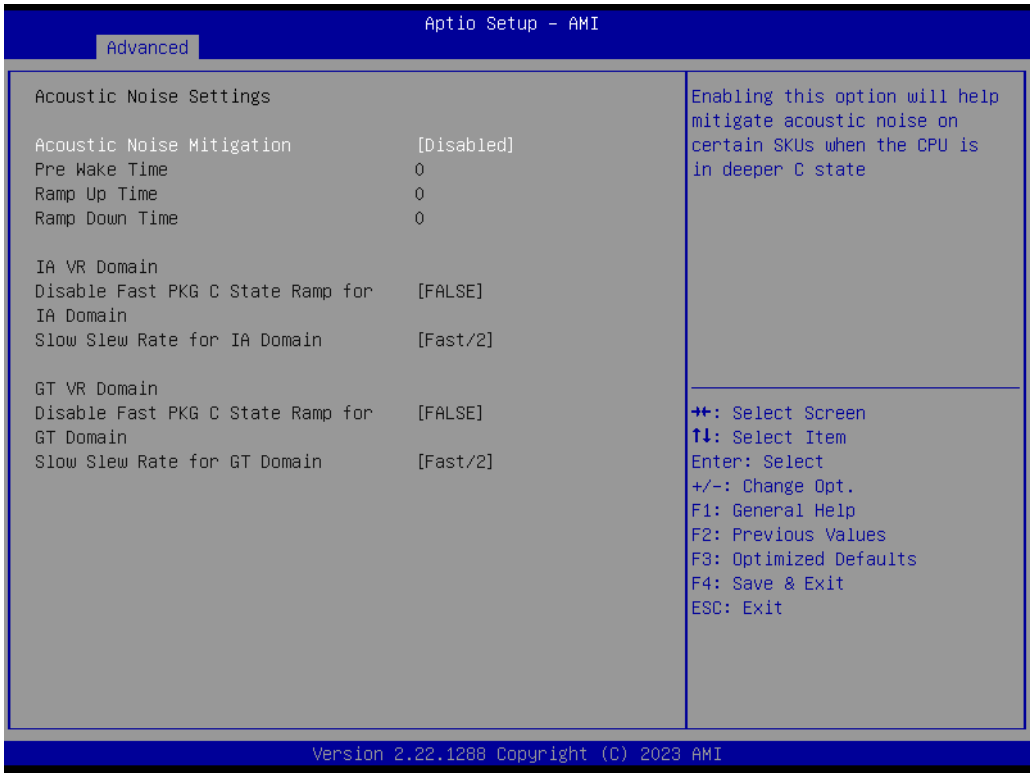
```
Aptio Setup - AMI
Advanced

CPU - Power Management Control                    CPU VR Settings

Boot performance mode              [Turbo Performance]
Intel(R) SpeedStep(tm)             [Enabled]
Race To Halt (RTH)                 [Enabled]
Intel(R) Speed Shift Technology    [Enabled]
Per Core P State OS control mode   [Enabled]
HwP Autonomous Per Core P State    [Enabled]
HwP Autonomous EPP Grouping        [Enabled]
EPB override over PECI             [Disabled]
HwP Lock                           [Enabled]
HDC Control                        [Enabled]
  Turbo Mode                       [Enabled]
▶ View/Configure Turbo Options                    →←: Select Screen
▶ CPU VR Settings                                 ↑↓: Select Item
Platform PL1 Enable                [Enabled]      Enter: Select
Platform PL1 Power                 27000          +/-: Change Opt.
Platform PL1 Time Window           [0]            F1: General Help
Platform PL2 Enable                [Enabled]      F2: Previous Values
Platform PL2 Power                 45000          F3: Optimized Defaults
ATX Telemetry Unit                 [Watts]        F4: Save & Exit
Power Limit 4 Override             [Enabled]      ESC: Exit
Power Limit 4                      60000
Power Limit 4 Lock                 [Disabled]
C states                           [Disabled]

Version 2.22.1288 Copyright (C) 2023 AMI
```

```
Aptio Setup - AMI
Advanced

CPU VR Settings                                   PSYS Slope defined in 1/100
                                                  increments. Range is 0-200.
Current VccIn Aux Icc Max          144            For a 1.25 slope, enter 125. 0
PSYS Slope                         0              = AUTO. Uses BIOS VR mailbox
PSYS Offset                        0              command 0x9.
  PSYS Prefix                      [+]
PSYS PMax Power                    0
Min Voltage Override               [Disabled]
VccIn Aux Icc Max                  0
VccIn Aux IMON Slope               100
VccIN Aux IMON Offset              0
  VccIN Aux IMON Prefix            [+]
Vsys/Psys Critical                 [Disabled]
Assertion Deglitch Mantissa        1              →←: Select Screen
Assertion Deglitch Exponent        0              ↑↓: Select Item
De assertion Deglitch Mantissa     13             Enter: Select
De assertion Deglitch Exponent     2              +/-: Change Opt.
VR Power Delivery Design           [AUTO]         F1: General Help
▶ Acoustic Noise Settings                         F2: Previous Values
▶ Core/IA VR Settings                             F3: Optimized Defaults
▶ GT VR Settings                                  F4: Save & Exit
▶ RFI Settings                                    ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

- **PSYS Slope**
  PSYS Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x9.
- **PSYS Offset**
  PSYS Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. PSYS Uses BIOS VR mailbox command 0x4.

- **PSYS prefix**
  Sets the offset value as positive or negative.
- **PSYS PMax Power**
  PSYS PMax power, defined in 1/8 Watt increments. Range 0-8191. For a PMax of 125W, enter 1000. 0 = AUTO. Uses BIOS VR mailbox command 0xB.
- **Min Voltage Override**
  Min Voltage Override. Enable to override minimum voltage for runtime and for C8.
- **VccIn Aux Icc Max**
  Sets the Max Icc VccIn Aux value defined in 1/4A increments. Range is 0-512. For an IccMax 32A, enter 128(32*4).
- **VccIn Aux IMON Slope**
  VccIN Aux IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x18.
- **VccIn Aux IMON Offset**
  VccIN Aux IMON Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. IMON Uses BIOS VR mailbox command 0x18.
- **VccIN Aux IMON Prefix**
  Sets the offset value as positive or negative.
- **Vsys Critical**
  Vsys Critical Enable or disable.
- **VR Power Delivery Design**
  Specifies the ADL Desktop board design used for the VR settings override values. By default, BIOS will override the default Desktop VR settings based on the board design. A value of AUTO(0) will use the board ID to determine the board design. Any other value will override the board ID logic to provide a custom VR Power Delivery Design value. This is intended primarily for validation.

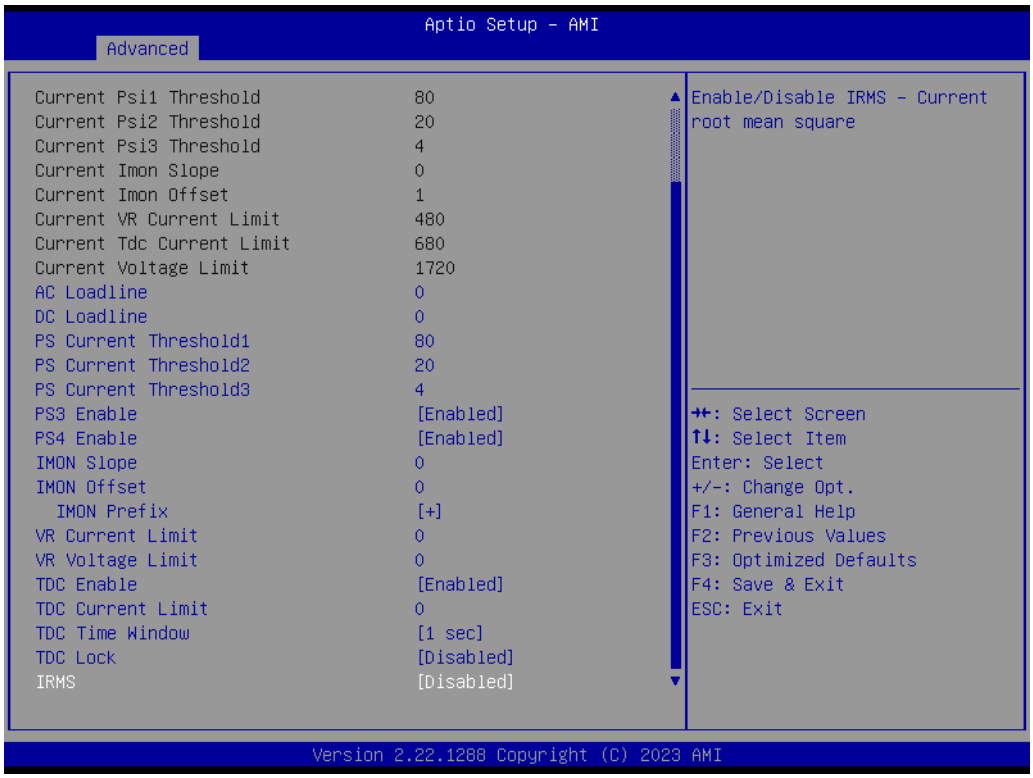




- **Acoustic Noise Mitigation**
  Enabling this option will help mitigate acoustic noise on certain SKUs when the CPU is in deeper C state.
- **Pre Wake time**
  Set the maximum Pre Wake randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Perodicity Alteration (DPA) tuning.
- **Ramp Up Time**
  Set the maximum Ramp Up randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Perodicity Alteration (DPA) tuning.
- **Ramp Down Time**
  Set the maximum Ramp Down randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Perodicity Alteration (DPA) tuning.
- **Disable Fast PKG C State Ramp for IA Domain**
  This option needs to be configured to reduce acoustic noise during deeper C states. False: Don't disable Fast ramp during deeper C states; True: Disable Fast ramp during deeper C state.
- **Slow Slew Rate for IA Domain**
  Set VR IA Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number, the number is 2, 4, 8, 16 to slow down the slew rate to help minimize acoustic noise.
- **Disable Fast PKG C State Ramp for GT Domain**
  This option needs to be configured to reduce acoustic noise during deeper C states. False: Don't disable Fast ramp during deeper C states; True: Disable Fast ramp during deeper C state.
- **Slow Slew Rate for GT Domain**
  Set VR GT Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number, the number is 2, 4, 8 to slow down the slew rate to help minimize acoustic noise; divide by 16 is disabled.

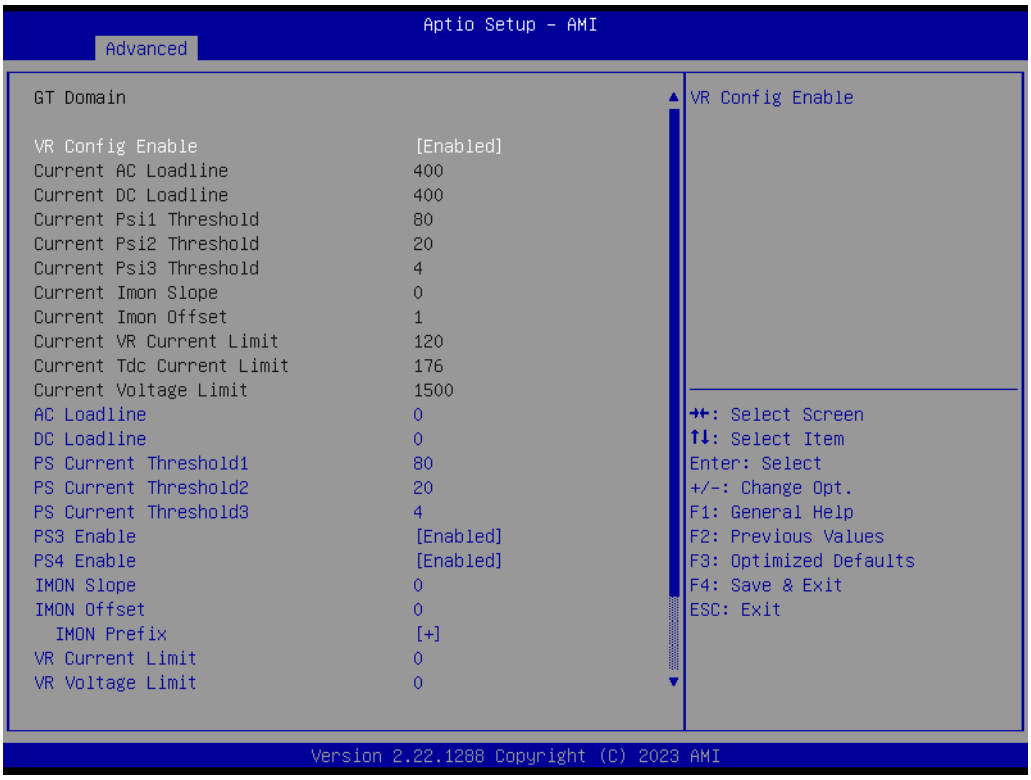
```
Aptio Setup - AMI
Advanced

CPU VR Settings                                   Core/IA VR Settings

Current VccIn Aux Icc Max            144
PSYS Slope                           0
PSYS Offset                          0
  PSYS Prefix                        [+]
PSYS PMax Power                      0
Min Voltage Override                 [Disabled]
VccIn Aux Icc Max                    0
VccIn Aux IMON Slope                 100
VccIN Aux IMON Offset                0
  VccIN Aux IMON Prefix              [+]
Vsys/Psys Critical                   [Disabled]
Assertion Deglitch Mantissa          1
Assertion Deglitch Exponent          0
De assertion Deglitch Mantissa       13
De assertion Deglitch Exponent       2
VR Power Delivery Design             [AUTO]
▶ Acoustic Noise Settings                         →←: Select Screen
▶ Core/IA VR Settings                             ↑↓: Select Item
▶ GT VR Settings                                  Enter: Select
▶ RFI Settings                                    +/-: Change Opt.
                                                  F1: General Help
                                                  F2: Previous Values
                                                  F3: Optimized Defaults
                                                  F4: Save & Exit
                                                  ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

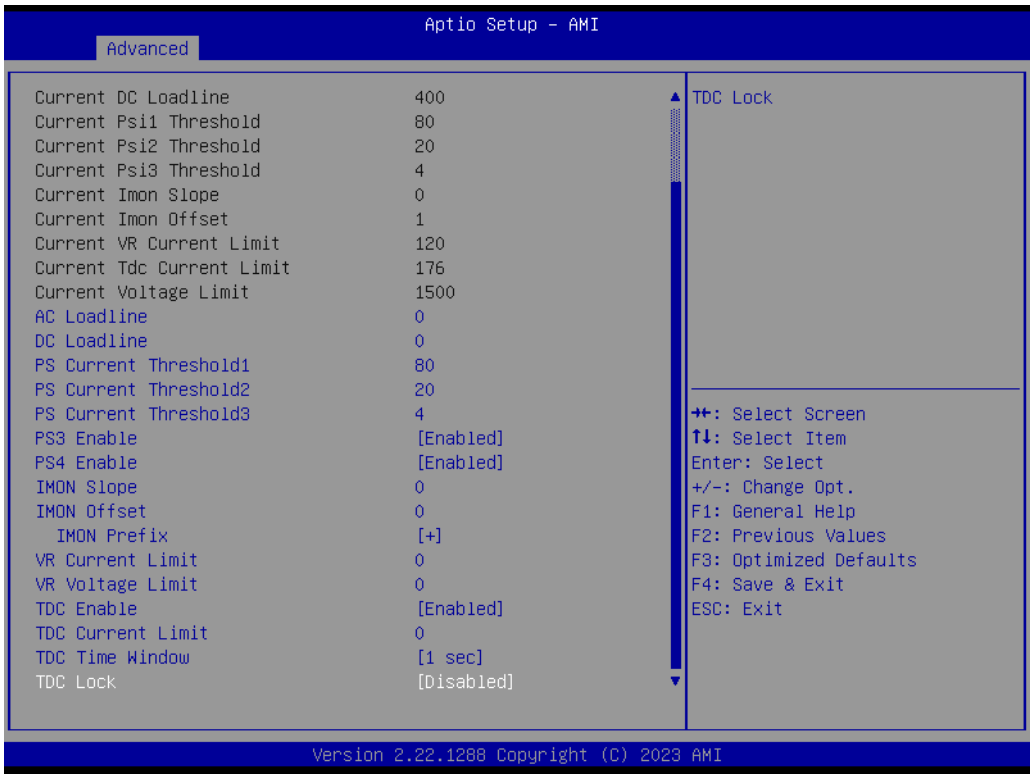
```
Aptio Setup - AMI
Advanced

Core/IA VR Domain                                 VR Config Enable

VR Config Enable                     [Enabled]
Current AC Loadline                  170
Current DC Loadline                  170
Current Psi1 Threshold               80
Current Psi2 Threshold               20
Current Psi3 Threshold               4
Current Imon Slope                   0
Current Imon Offset                  1
Current VR Current Limit             480
Current Tdc Current Limit            680
Current Voltage Limit                1720
AC Loadline                          0
DC Loadline                          0
PS Current Threshold1                80
PS Current Threshold2                20
PS Current Threshold3                4
PS3 Enable                           [Enabled]
PS4 Enable                           [Enabled]
IMON Slope                           0
IMON Offset                          0
  IMON Prefix                        [+]
VR Current Limit                     0
VR Voltage Limit                     0                →←: Select Screen
                                                      ↑↓: Select Item
                                                      Enter: Select
                                                      +/-: Change Opt.
                                                      F1: General Help
                                                      F2: Previous Values
                                                      F3: Optimized Defaults
                                                      F4: Save & Exit
                                                      ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```



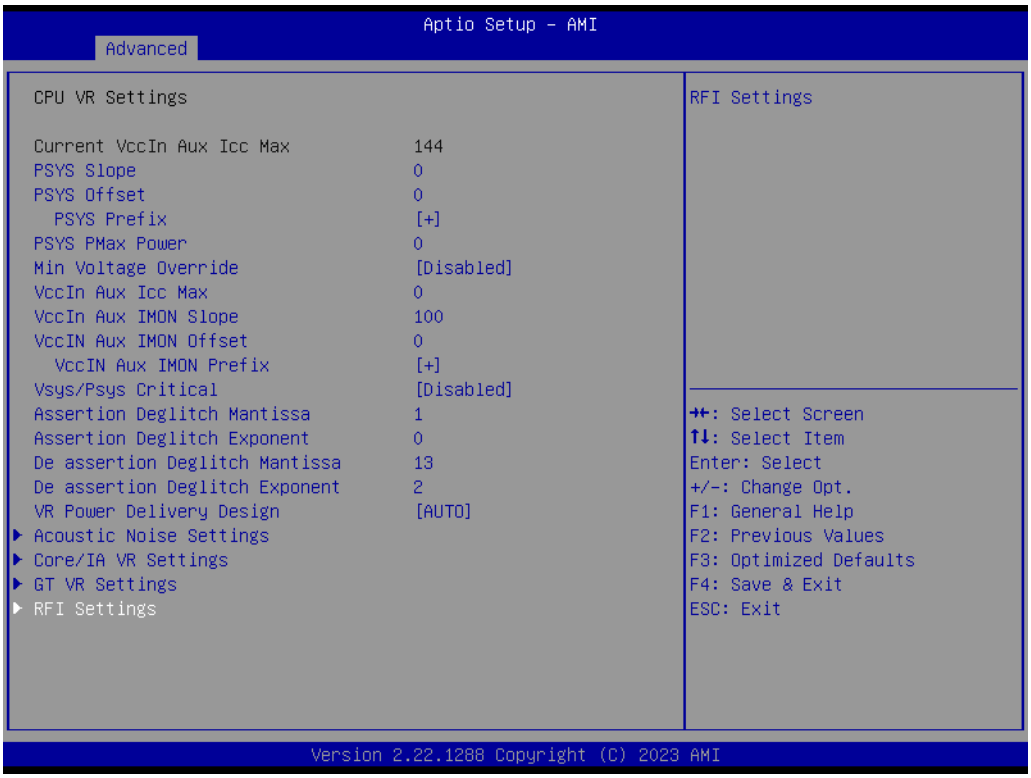
- **VR Config Enable**
  VR Config Enable.
- **PS3 Enable**
  PS3 Enable/Disable. 0 - Disabled, 1 - Enabled.Uses BIOS VR mailbox command 0x3.
- **PS4 Enable**
  PS4 Enable/Disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3.
- **IMON Prefix**
  Sets the offset value as positive or negative.

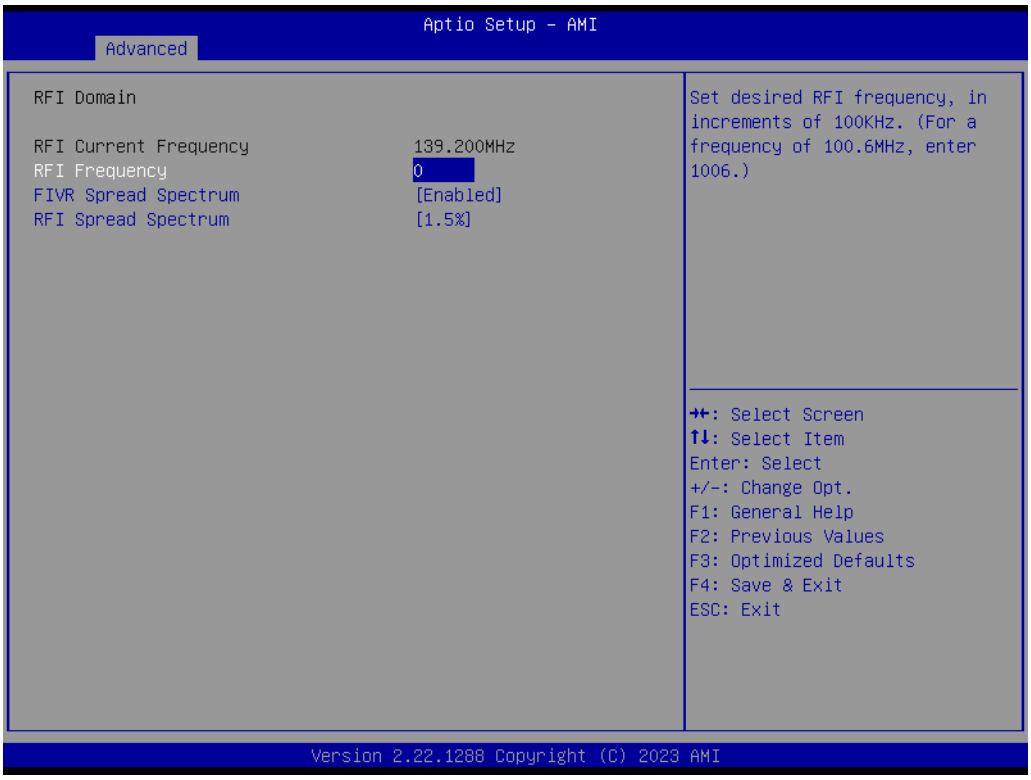
Aptio Setup - AMI
Advanced
CPU VR Settings
Current VccIn Aux Icc Max 144
PSYS Slope 0
PSYS Offset 0
PSYS Prefix [+]
PSYS PMax Power 0
Min Voltage Override [Disabled]
VccIn Aux Icc Max 0
VccIn Aux IMON Slope 100
VccIN Aux IMON Offset 0
VccIN Aux IMON Prefix [+]
Vsys/Psys Critical [Disabled]
Assertion Deglitch Mantissa 1
Assertion Deglitch Exponent 0
De assertion Deglitch Mantissa 13
De assertion Deglitch Exponent 2
VR Power Delivery Design [AUTO]
Acoustic Noise Settings
Core/IA VR Settings
GT VR Settings
RFI Settings
GT VR Settings
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.22.1288 Copyright (C) 2023 AMI


Aptio Setup - AMI
Advanced
GT Domain
VR Config Enable [Enabled]
Current AC Loadline 400
Current DC Loadline 400
Current Psi1 Threshold 80
Current Psi2 Threshold 20
Current Psi3 Threshold 4
Current Imon Slope 0
Current Imon Offset 1
Current VR Current Limit 120
Current Tdc Current Limit 176
Current Voltage Limit 1500
AC Loadline 0
DC Loadline 0
PS Current Threshold1 80
PS Current Threshold2 20
PS Current Threshold3 4
PS3 Enable [Enabled]
PS4 Enable [Enabled]
IMON Slope 0
IMON Offset 0
IMON Prefix [+]
VR Current Limit 0
VR Voltage Limit 0
VR Config Enable
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.22.1288 Copyright (C) 2023 AMI



- **VR Config Enable**
  VR Config Enable.
- **PS3 Enable**
  PS3 Enable/Disable. 0 - Disabled, 1 - Enabled.Uses BIOS VR mailbox command 0x3.
- **PS4 Enable**
  PS4 Enable/Disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3.





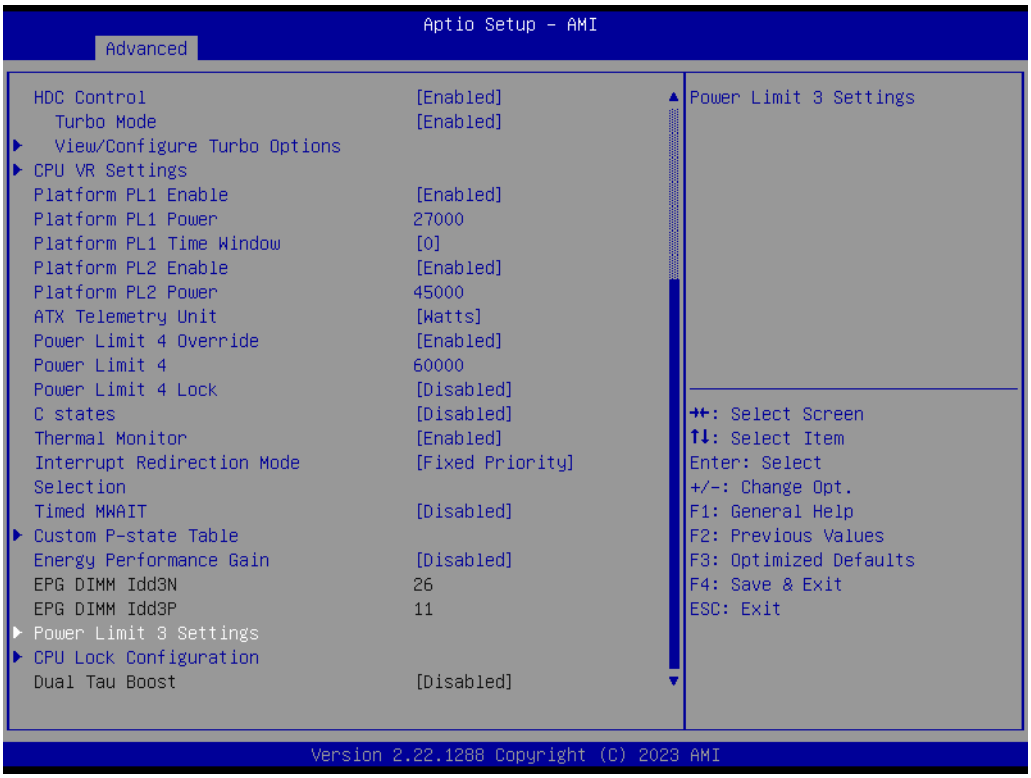
- **FIVR Spread Spectrum**
  Enable or Disable the FIVR Spread Spectrum.
- **RFI Spread Spectrum**
  Set the Spread Spectrum.

```
Aptio Setup - AMI
Advanced

HDC Control                          [Enabled]
  Turbo Mode                         [Enabled]
▶ View/Configure Turbo Options
▶ CPU VR Settings
Platform PL1 Enable                  [Enabled]
Platform PL1 Power                   27000
Platform PL1 Time Window             [0]
Platform PL2 Enable                  [Enabled]
Platform PL2 Power                   45000
ATX Telemetry Unit                   [Watts]
Power Limit 4 Override               [Enabled]
Power Limit 4                        60000
Power Limit 4 Lock                   [Disabled]
C states                             [Disabled]
Thermal Monitor                      [Enabled]
Interrupt Redirection Mode           [Fixed Priority]
Selection
Timed MWAIT                          [Disabled]
▶ Custom P-state Table
Energy Performance Gain              [Disabled]
EPG DIMM Idd3N                       26
EPG DIMM Idd3P                       11
▶ Power Limit 3 Settings
▶ CPU Lock Configuration
Dual Tau Boost                       [Disabled]

Add Custom P-state Table

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

```
Aptio Setup - AMI
Advanced

Custom P-state Table

Number of P states                   0

Sets the number of custom
P-states. At least 2 states
must be present.

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

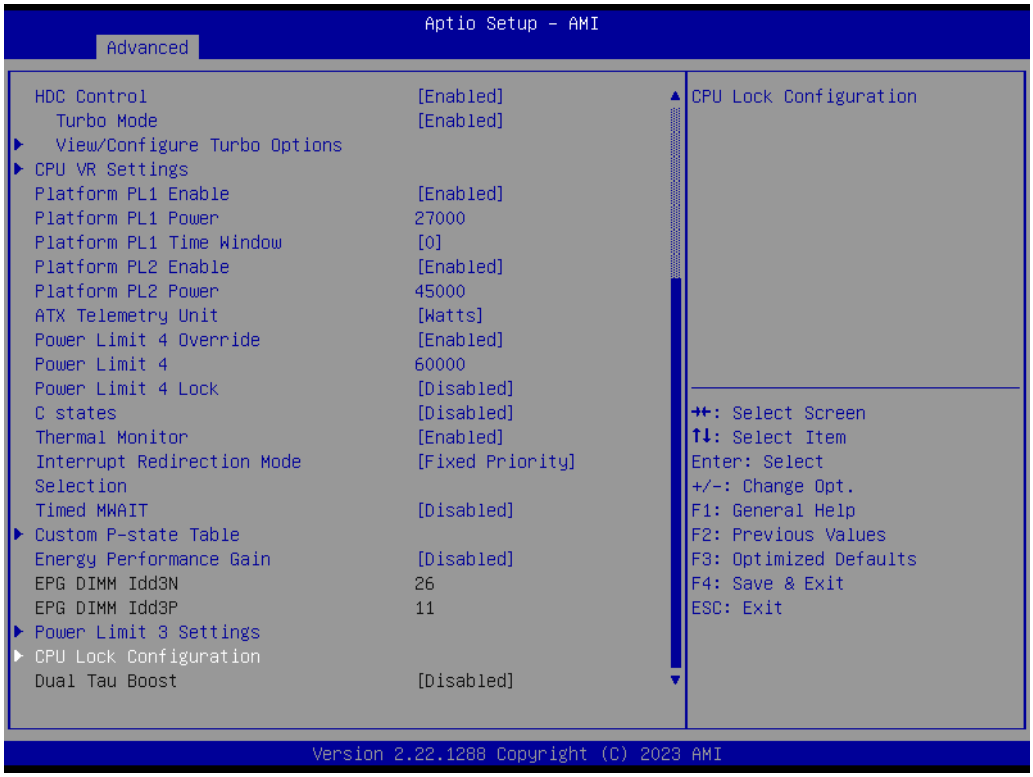
■ **Number of P states**

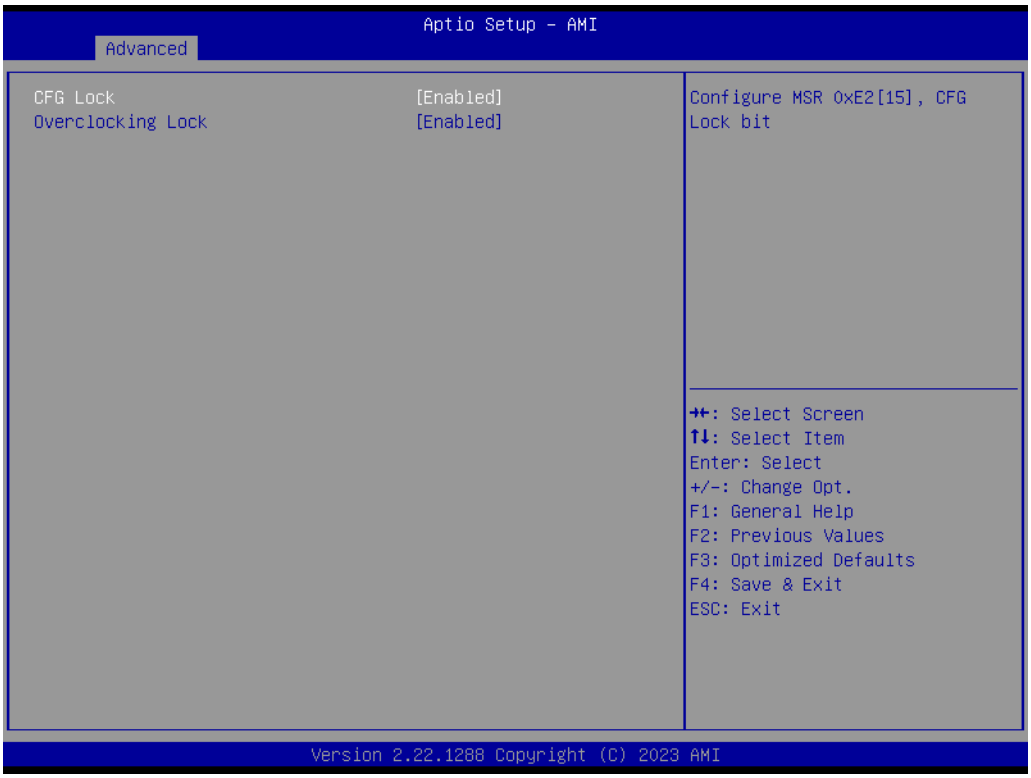
Sets the number of custom P-states. At least 2 states must be present.



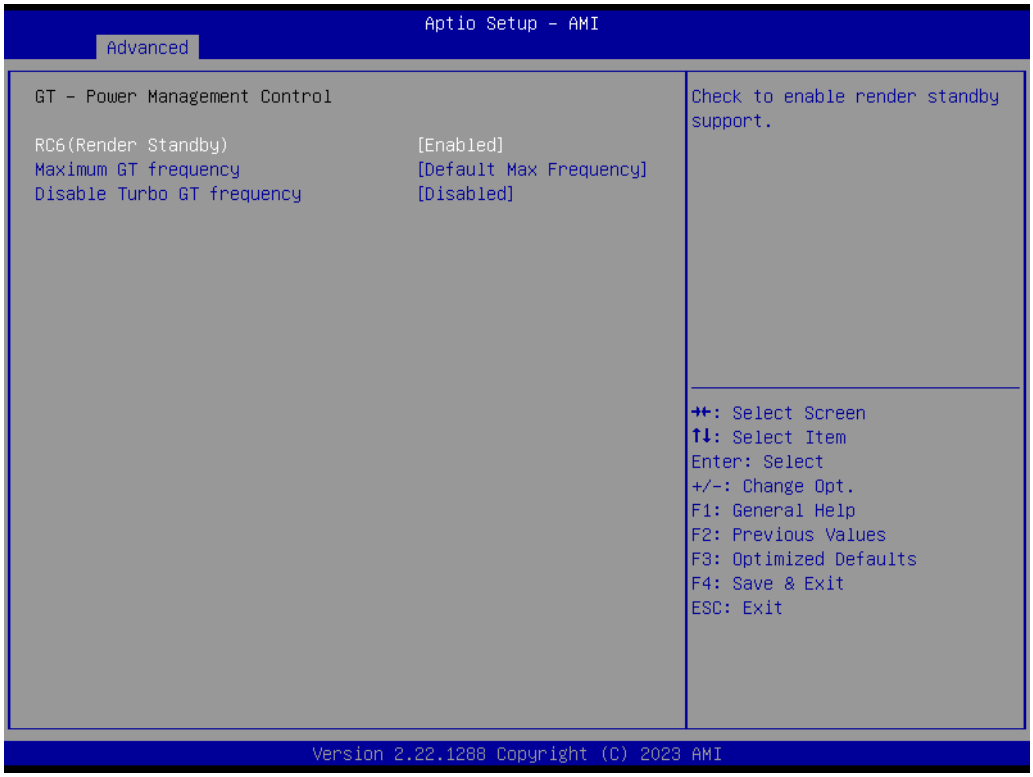
- **Power Limit 3 Override**
  Enable/Disable Power Limit 3 override.
- **Power Limit 3**
  Power Limit 3 in milliwatts.
- **Power Limit 3 Time Window**
  Power Limit 3 Time Window value in milliseconds.

- **Power Limit 3 Duty Cycle**
  Specify the duty cycle in percentage that the CPU is required to maintain over the configured time window. Range is 0-100.
- **Power Limit 3 Lock**
  Power Limit 3 MSR 615h Lock. When enabled, PL3 configurations are locked during OS. When disabled PL3 configuration can be changed during OS.





- **CFG Lock**
  Configure MSR 0xE2[15], CFG Lock bit.
- **Overclocking Lock**
  Enable/Disable Overclocking Lock (BIT 20) in FLEX_RATIO(194) MSR.



- **RC6 (Render Standby)**
  Check to enable render standby support.
- **Maximum GT frequency**
  Maximum GT frequency limited by the user.
- **Disable Turbo GT frequency**
  Enabled: Disables Turbo GT frequency. Disabled: GT frequency is not limited.

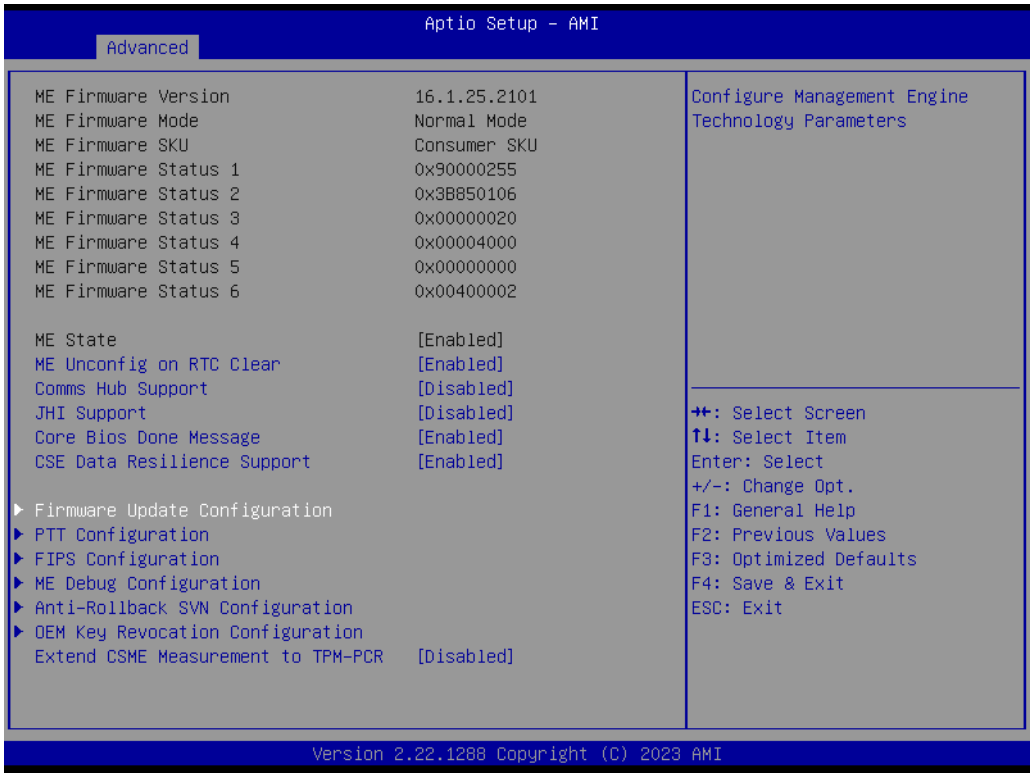
3.2.2.3 PCH-FW Configuration

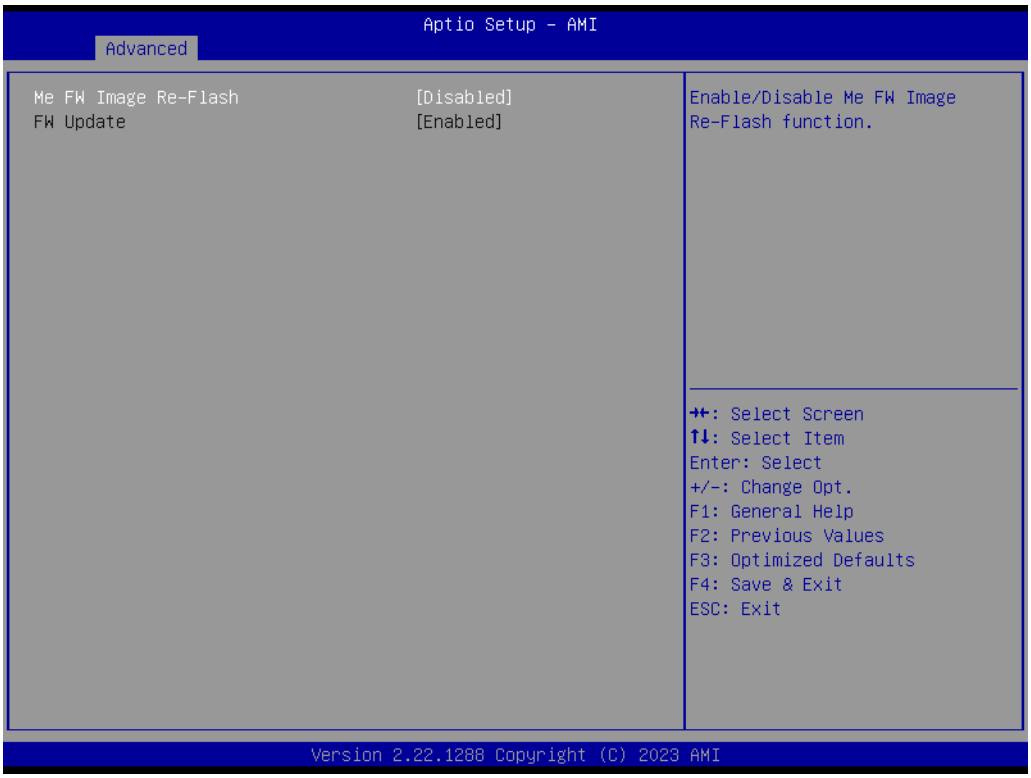
```
Aptio Setup - AMI
Main  Advanced  Chipset  Security  Boot  Save & Exit  NVMe RPMB Key Migration

▶ CPU Configuration                          Configure Management Engine
▶ Power & Performance                        Technology Parameters
▶ PCH-FW Configuration
▶ ACPI Settings
▶ NCT6126D Super IO Configuration
▶ iManager Configuration
▶ S5 RTC Wake Settings
▶ Serial Port Console Redirection
▶ USB Configuration
▶ Network Stack Configuration
▶ CSM Configuration
▶ NVMe Configuration

▶ Tls Auth Configuration                     →←: Select Screen
                                             ↑↓: Select Item
▶ Driver Health                              Enter: Select
                                             +/-: Change Opt.
                                             F1: General Help
                                             F2: Previous Values
                                             F3: Optimized Defaults
                                             F4: Save & Exit
                                             ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

```
Aptio Setup - AMI
Advanced

ME Firmware Version                16.1.25.2101      When Disabled ME will not be
ME Firmware Mode                   Normal Mode       unconfigured on RTC Clear
ME Firmware SKU                    Consumer SKU
ME Firmware Status 1               0x90000255
ME Firmware Status 2               0x3B850106
ME Firmware Status 3               0x00000020
ME Firmware Status 4               0x00004000
ME Firmware Status 5               0x00000000
ME Firmware Status 6               0x00400002

ME State                           [Enabled]
ME Unconfig on RTC Clear           [Enabled]
Comms Hub Support                  [Disabled]
JHI Support                        [Disabled]        →←: Select Screen
Core Bios Done Message             [Enabled]         ↑↓: Select Item
CSE Data Resilience Support        [Enabled]         Enter: Select
                                                     +/-: Change Opt.
▶ Firmware Update Configuration                      F1: General Help
▶ PTT Configuration                                  F2: Previous Values
▶ FIPS Configuration                                 F3: Optimized Defaults
▶ ME Debug Configuration                             F4: Save & Exit
▶ Anti-Rollback SVN Configuration                    ESC: Exit
▶ OEM Key Revocation Configuration
Extend CSME Measurement to TPM-PCR [Disabled]

Version 2.22.1288 Copyright (C) 2023 AMI
```

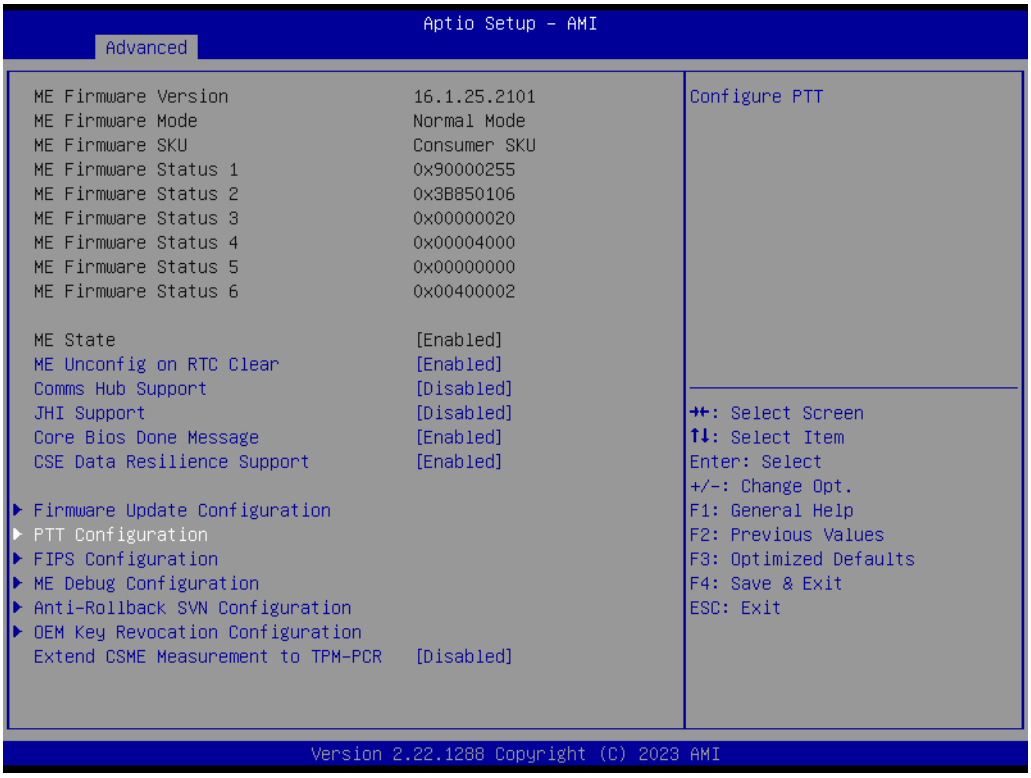
- **ME State**
  When Disabled, ME will be put into ME Temporarily Disabled Mode.
- **Manageability Features State**
  Enable/Disable Intel Manageability features.

- **AMT BIOS Features**
  When disabled, AMT BIOS Features are no longer supported and the user is no longer able to access MEBx Setup.
- **ME Unconfig on RTC Clear**
  When Disabled, ME will not be unconfigured on RTC Clear.
- **Comms hub support**
  Enables/Disables support for Comms Hub.
- **JHI support**
  Enable/Disable Intel® DAL Host Interface Service (JHI).
- **Core BIOS Done Message**
  Enable/Disable Core BIOS Done message sent to ME.





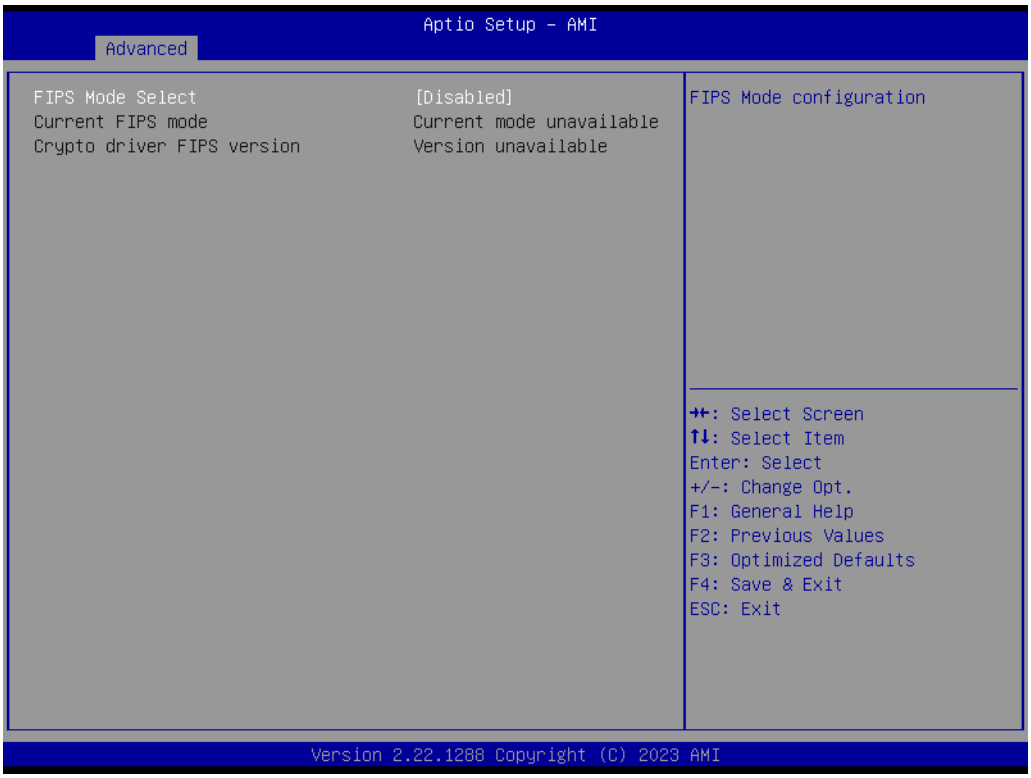
- **ME FW Image Re-Flash**
  Enable/Disable ME FW Image Re-Flash function.
- **FW Update**
  Enable/Disable ME FW Update function.



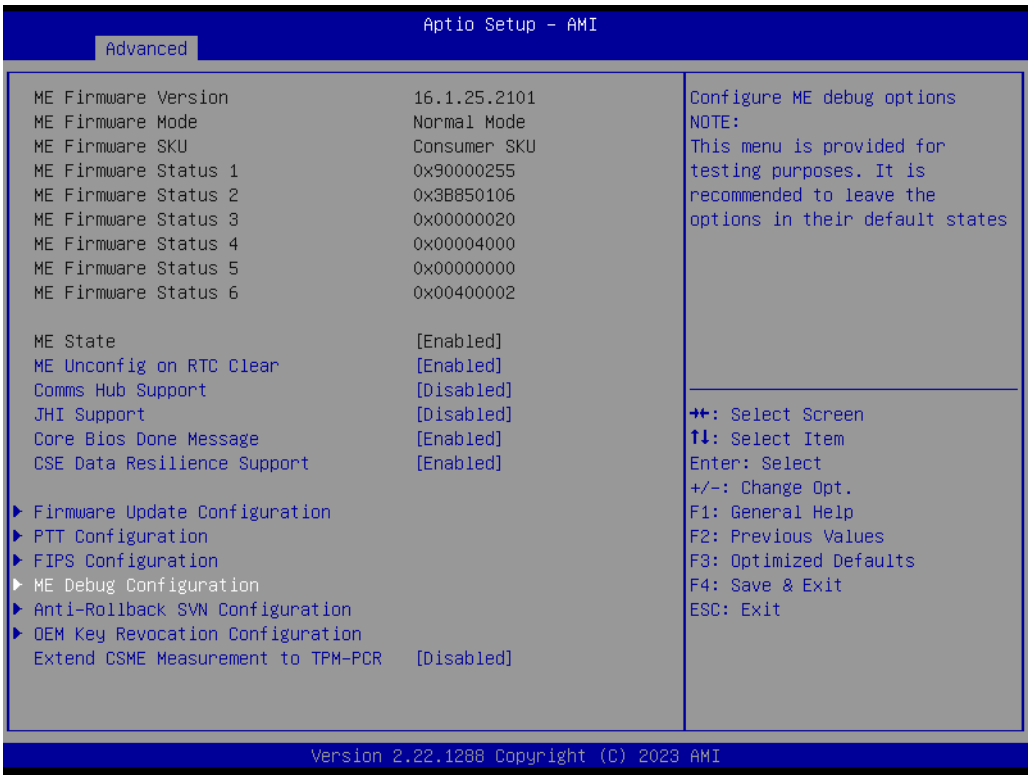
```
Aptio Setup - AMI
Advanced

PTT Capability / State          1 / 0

TPM Device Selection            [dTPM]

                                →←: Select Screen
                                ↑↓: Select Item
                                Enter: Select
                                +/-: Change Opt.
                                F1: General Help
                                F2: Previous Values
                                F3: Optimized Defaults
                                F4: Save & Exit
                                ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

■ **TPM Device Selection**
Configure TPM device.

```
Aptio Setup - AMI
Advanced

ME Firmware Version             16.1.25.2101        FIPS Mode help
ME Firmware Mode                Normal Mode
ME Firmware SKU                 Consumer SKU
ME Firmware Status 1            0x90000255
ME Firmware Status 2            0x3B850106
ME Firmware Status 3            0x00000020
ME Firmware Status 4            0x00004000
ME Firmware Status 5            0x00000000
ME Firmware Status 6            0x00400002

ME State                        [Enabled]
ME Unconfig on RTC Clear        [Enabled]
Comms Hub Support               [Disabled]
JHI Support                     [Disabled]          →←: Select Screen
Core Bios Done Message          [Enabled]           ↑↓: Select Item
CSE Data Resilience Support     [Enabled]           Enter: Select
                                                    +/-: Change Opt.
▶ Firmware Update Configuration                     F1: General Help
▶ PTT Configuration                                 F2: Previous Values
▶ FIPS Configuration                                F3: Optimized Defaults
▶ ME Debug Configuration                            F4: Save & Exit
▶ Anti-Rollback SVN Configuration                   ESC: Exit
▶ OEM Key Revocation Configuration
Extend CSME Measurement to TPM-PCR  [Disabled]

Version 2.22.1288 Copyright (C) 2023 AMI
```



■ **FIPS mode select**
FIPS mode configuration.

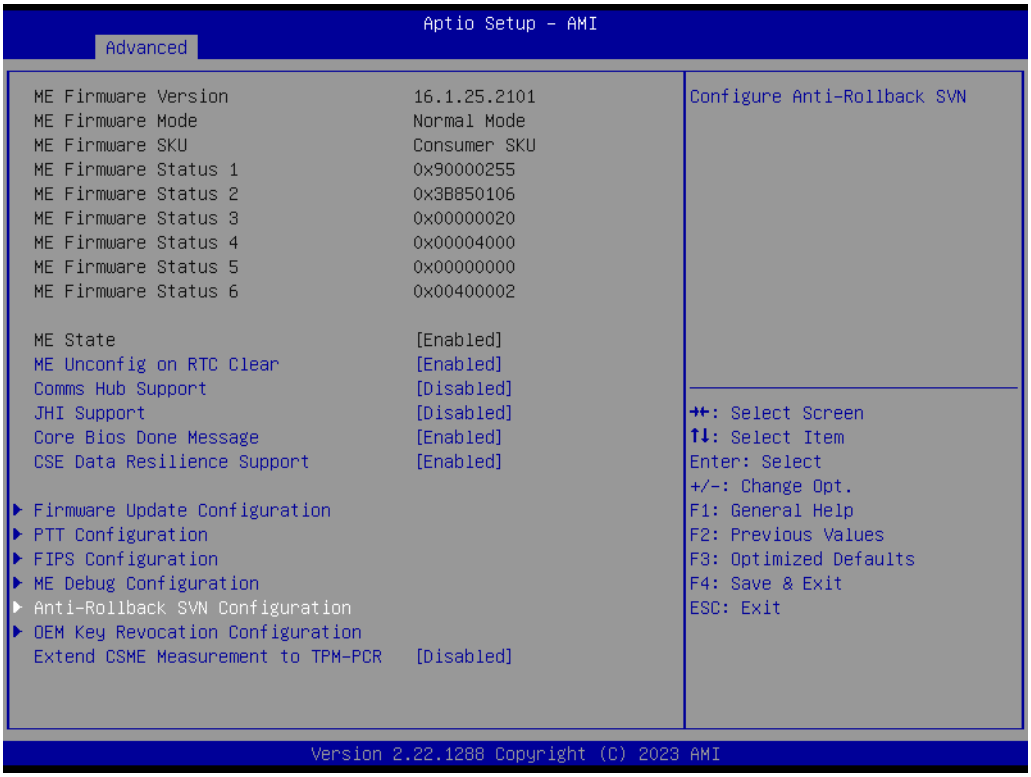


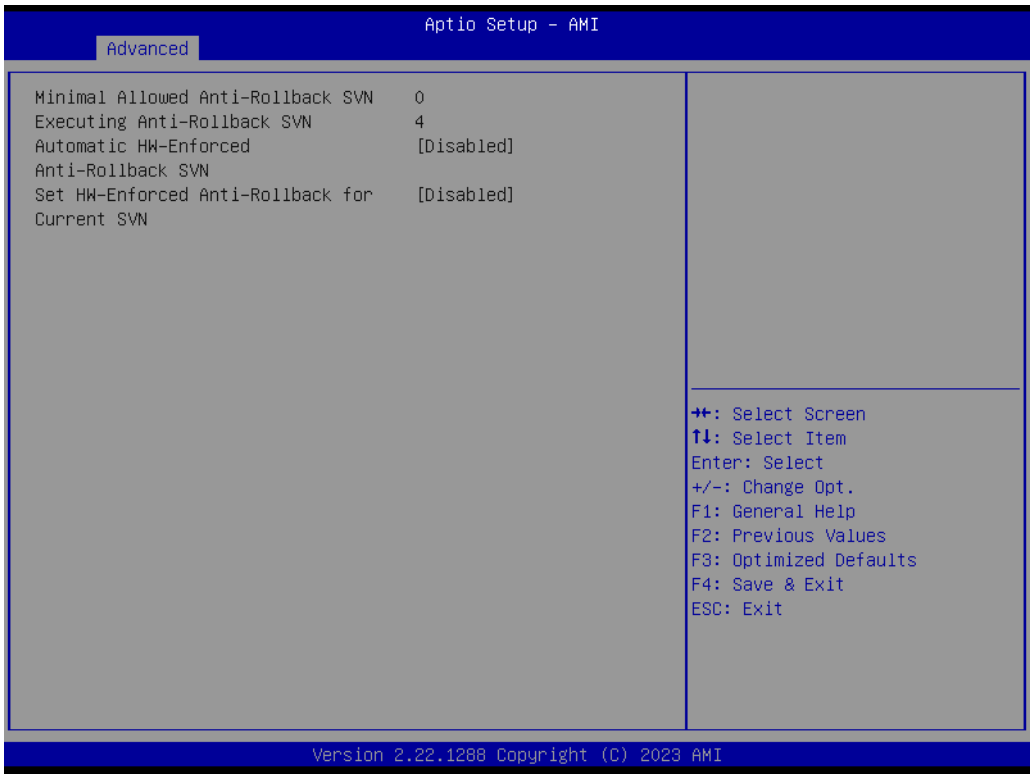
```
Aptio Setup - AMI
Advanced

HECI Timeouts                          [Enabled]

Force ME DID Init Status               [Disabled]
CPU Replaced Polling Disable           [Disabled]
HECI Message check Disable             [Disabled]
MBP HOB Skip                           [Disabled]
HECI2 Interface Communication          [Disabled]
KT Device                              [Enabled]
End Of Post Message                    [Send in DXE]
DOI3 Setting for HECI Disable          [Disabled]
MCTP Broadcast Cycle                   [Disabled]
▶ SMBIOS type 130 OEM capabilities

Enable/Disable HECI
Send/Receive Timeouts.

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

```
Aptio Setup - AMI
Advanced

BIOS Reflash Capability State          [Enabled]
BIOS Boot to Setup Capability          [Enabled]
State
BIOS Pause Before Booting              [Disabled]
Capability State
BIOS Secure Boot Capability            [Enabled]
Exposure to FW State

Change BIOS Reflash Capability
State

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

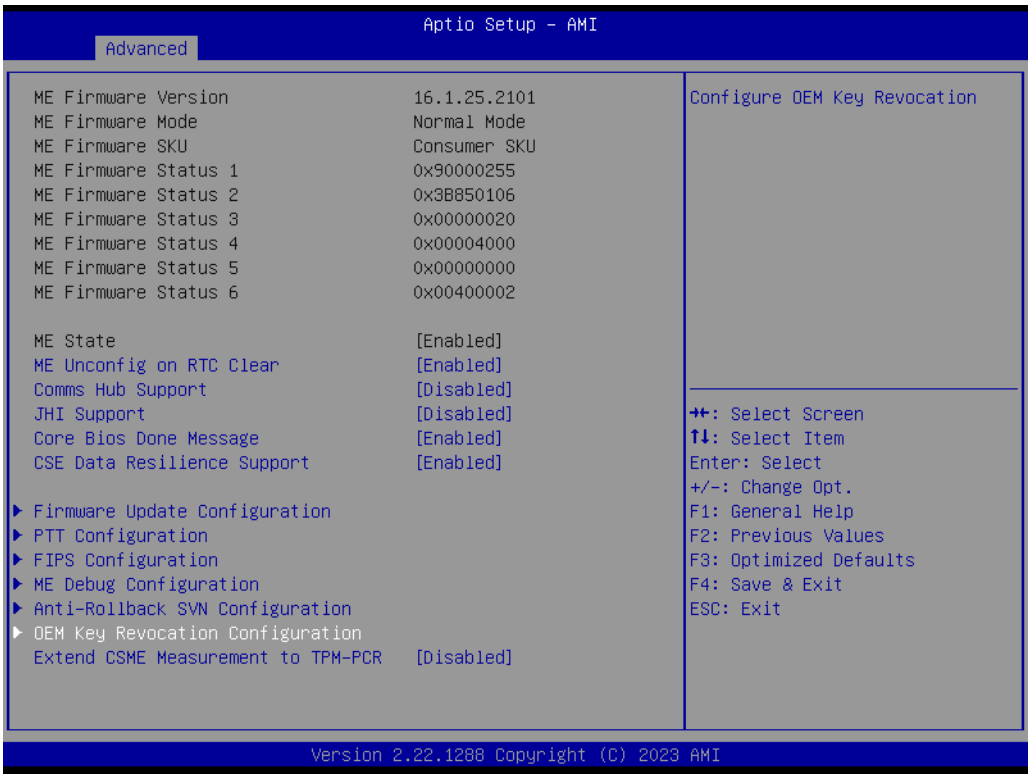
- **HECI Timeouts**
  Unique platform ID configuration.
- **Force ME DID Init Status**
  Unique platform ID configuration.
- **CPU Replaced Polling Disable**
  Setting this option disables the CPU replacement polling loop.

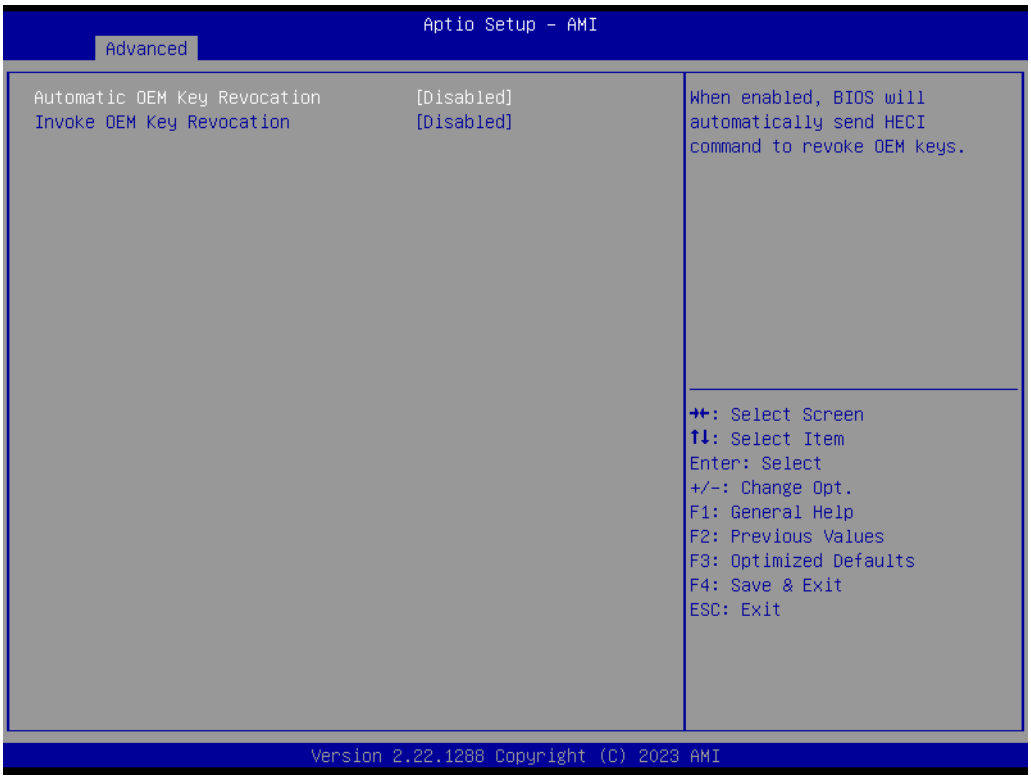
- **HECI Message check Disable**
  Setting this option disables message check for BIOS Boot Path when sending.
- **MBP HOB Skip**
  Setting this option will skip MBP HOB.
- **HECI2 Interface Communication**
  Adds and Removes HECI2 Device from PCI space.
- **KT Device**
  Enable/Disable KT Device.
- **End Of Post Message**
  Enable/Disable End of Post message sent to ME.
- **D0I3 Settings for HECI Disable**
  Setting this option disables setting D0I3 bit for all HECI devices.
- **MCTP Broadcast Cycle**
  Enable/Disable Management Component Transport Protocol Broadcast Cycle and Set PMT as Bus Owner.
- **BIOS Reflash Capability State**
  Change BIOS Reflash Capability State.
- **BIOS Boot to Setup Capability State**
  Change BIOS Boot to Setup Capability State.
- **BIOS Pause Before Booting Capability State**
  Change BIOS Pause Before Booting Capability State.
- **BIOS Secure Boot Capability Exposure to FW State**
  Change BIOS Secure Capability Exposure State to FW. This does not affect SecureBoot as such.





- **Automatic HW-Enforced Anti-Rollback SVN**
  When enabled, the hardware-enforced Anti-Rollback mechanism is automatically activated: once ME FW was successfully run on a platform, FW with lower ARB-SVN will be blocked from execution.
- **Set HW-Enforced Anti-Rollback for Current SVN**
  Enable the hardware-enforced Anti-Rollback mechanism for current ARB-SVN value. FW with lower ARB-SVN will be blocked from execution. The value will be restored to disable after the command is sent.

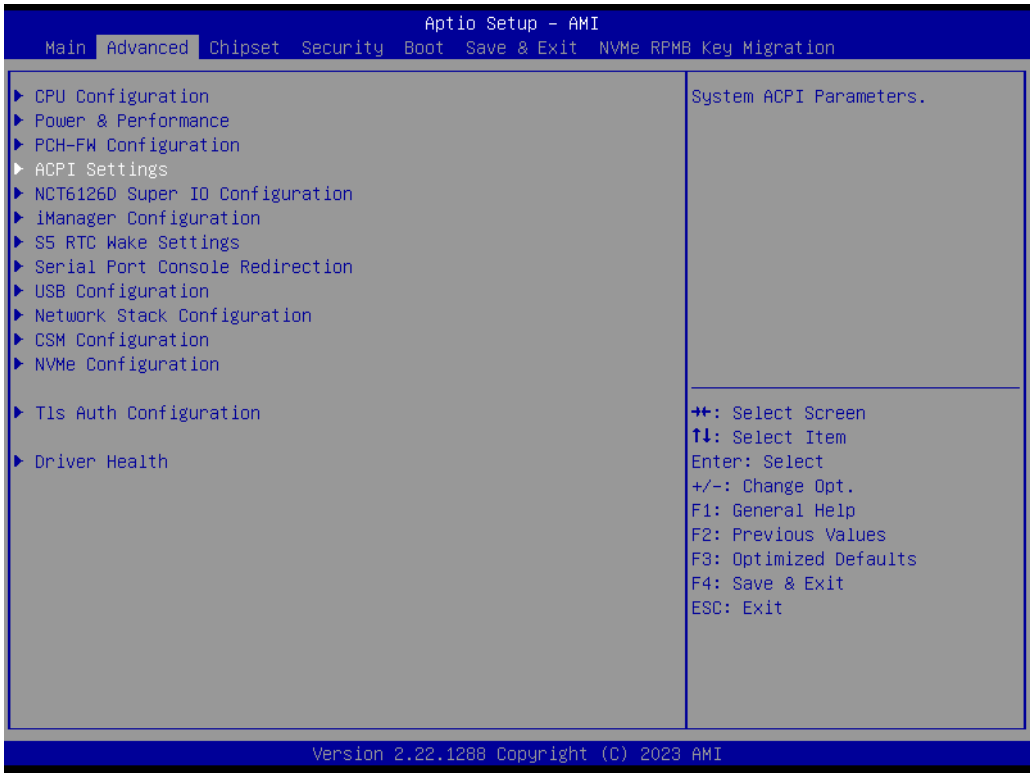


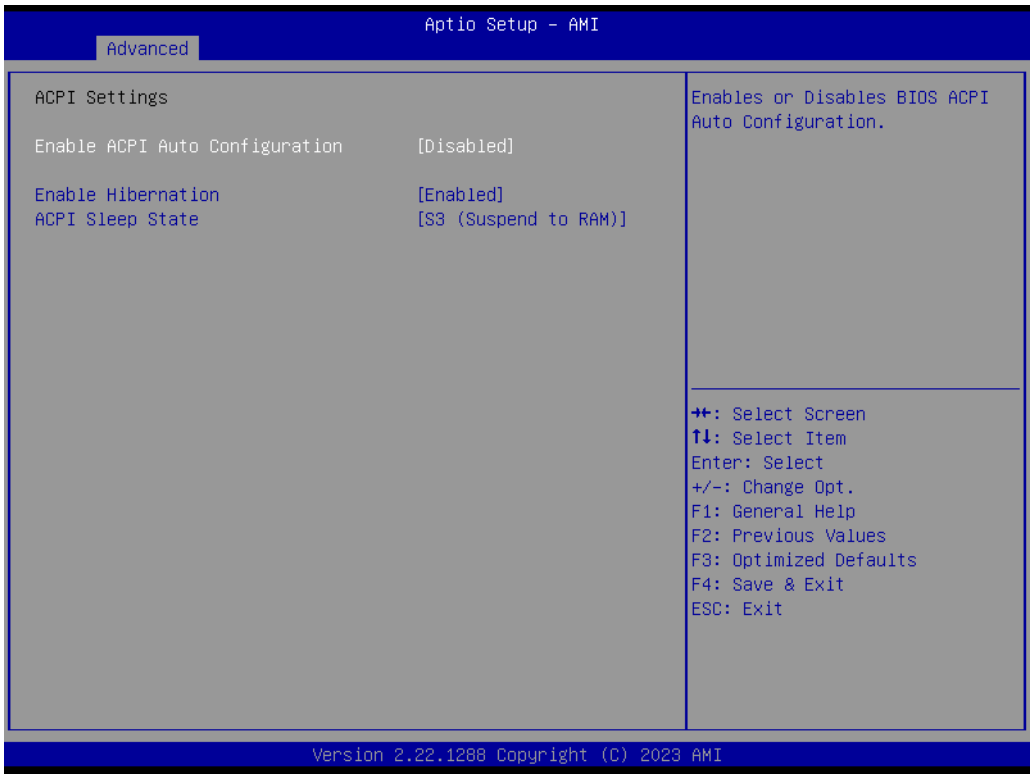


- **Automatic OEM Key Revocation**
  When enabled, the BIOS will automatically send HECI command to revoke OEM keys.
- **Invoke OEM Key Revocation**
  A Heci command will be sent to revoke the OEM key.

- **Extend CSME Measurement to TPM-PCR**
  Enable/Disable Extend CSME Measurement to TPM-PCR[0] and AMT Config to TPM-PCR[1].

3.2.2.4 ACPI Settings

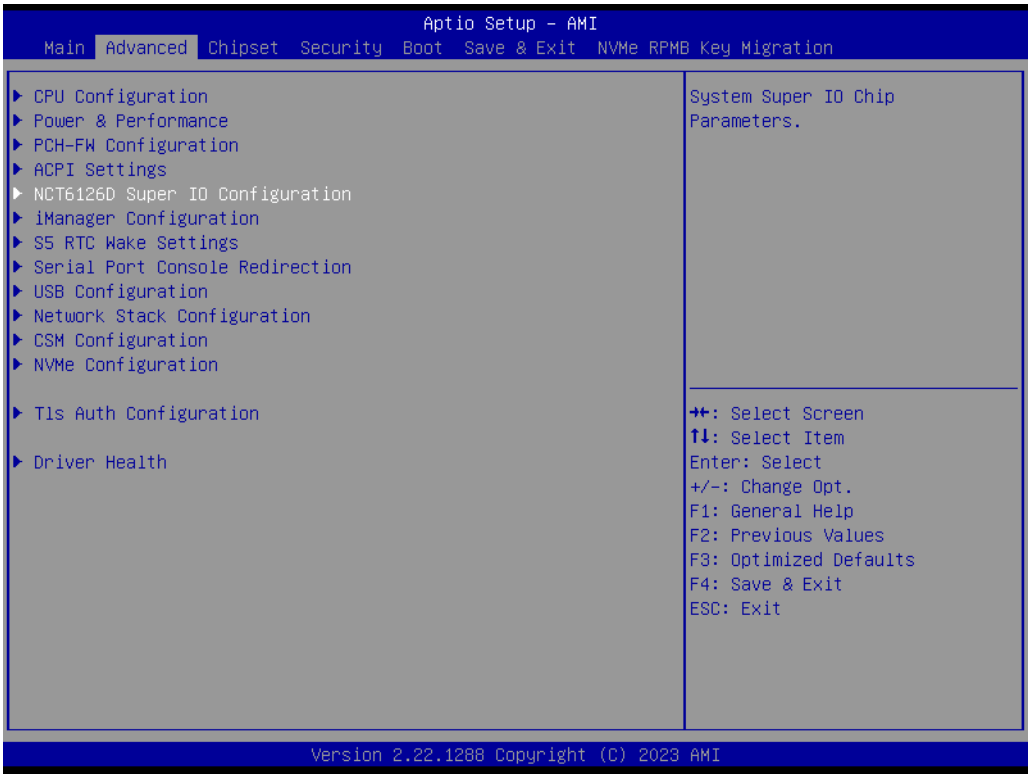


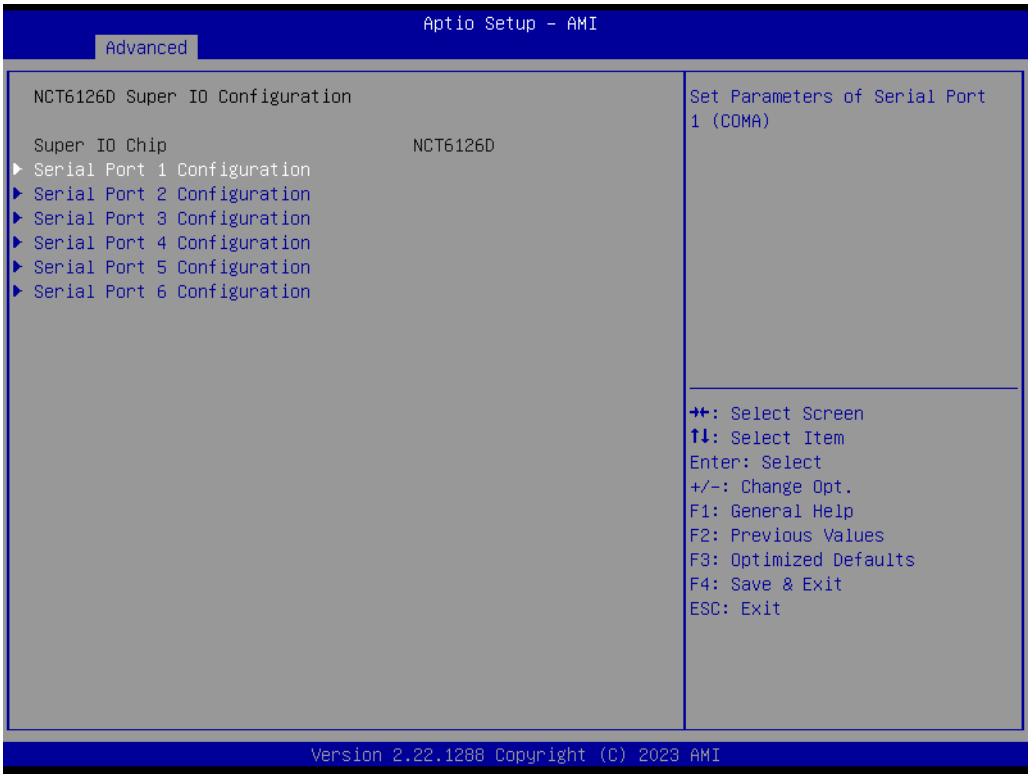


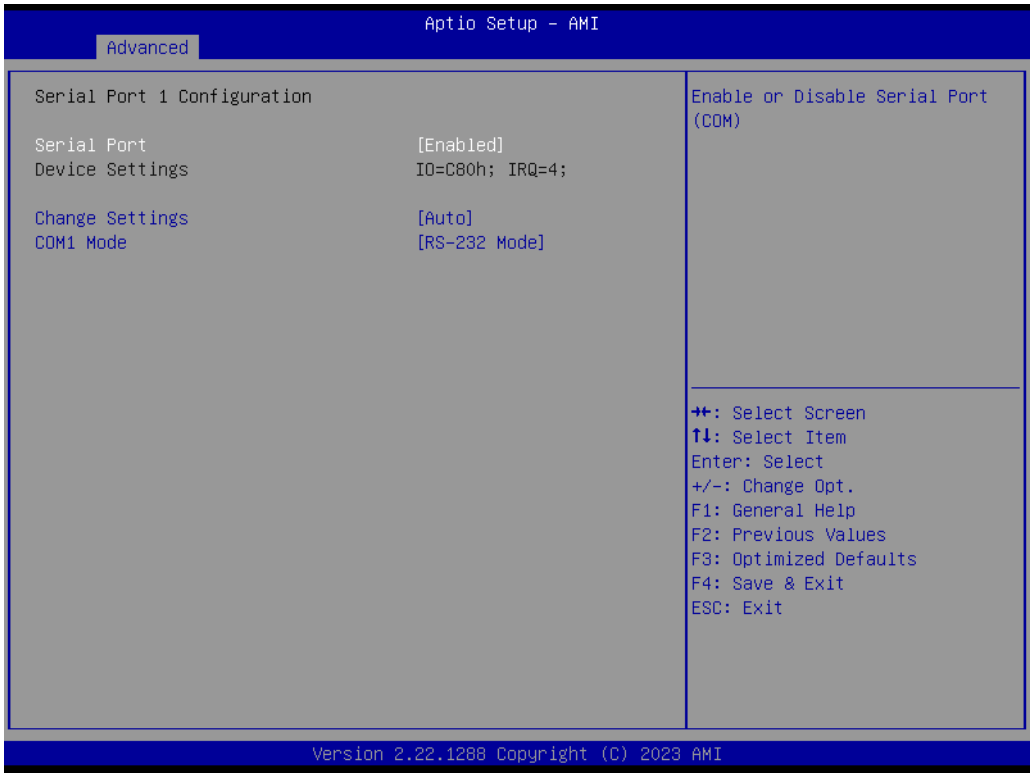
- **Enable ACPI Auto Configuration**
  Enables or Disables BIOS ACPI Auto Configuration.

- **Enable Hibernation**
  Enables or Disables System's ability to Hibernate (OS/S4 Sleep State).
- **ACPI Sleep State**
  Select the highest ACPI sleep state the system will enter when the SUSPEND button is pressed.

3.2.2.5 NCT61260 Super I/O Configuration







- **Serial Port**
  Enable or Disable Serial Port.
- **Change Settings**
  Select an optimal setting for super IO device.
- **COM3~6 Mode**
  COM Mode Select.

3.2.2.6 iManager Configuration

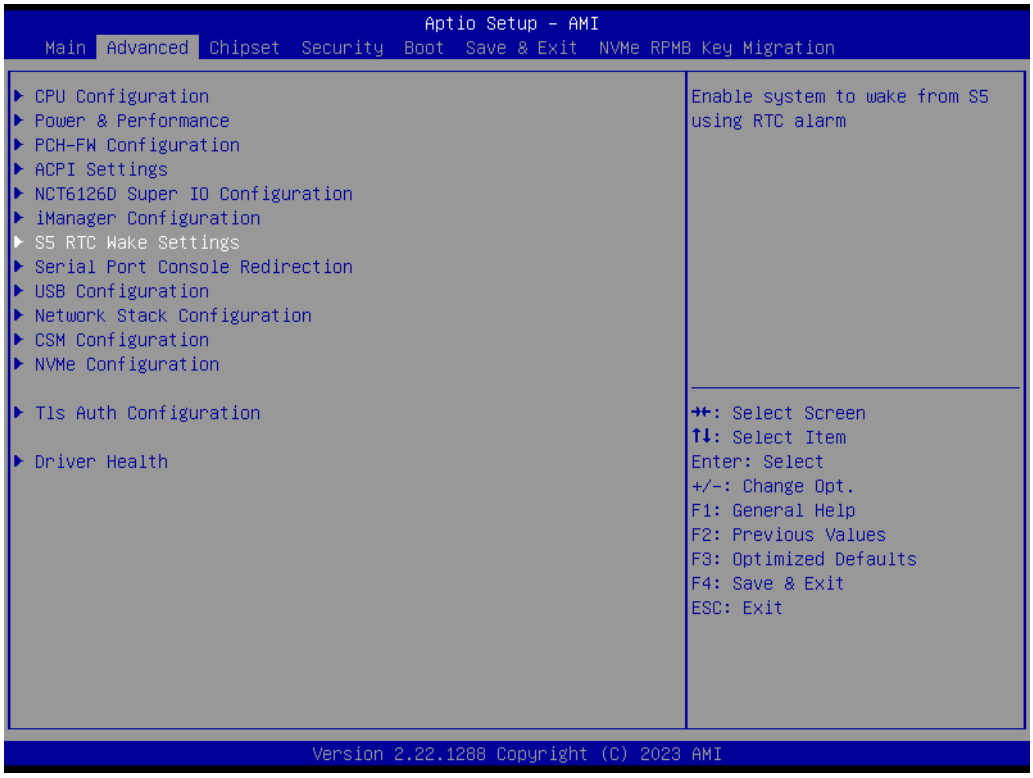
```
Aptio Setup - AMI
Main  Advanced  Chipset  Security  Boot  Save & Exit  NVMe RPMB Key Migration

▶ CPU Configuration                          iManager Parameters.
▶ Power & Performance
▶ PCH-FW Configuration
▶ ACPI Settings
▶ NCT6126D Super IO Configuration
▶ iManager Configuration
▶ S5 RTC Wake Settings
▶ Serial Port Console Redirection
▶ USB Configuration
▶ Network Stack Configuration
▶ CSM Configuration
▶ NVMe Configuration

▶ Tls Auth Configuration                     →←: Select Screen
                                             ↑↓: Select Item
▶ Driver Health                              Enter: Select
                                             +/-: Change Opt.
                                             F1: General Help
                                             F2: Previous Values
                                             F3: Optimized Defaults
                                             F4: Save & Exit
                                             ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

```
Aptio Setup - AMI
Advanced

iManager Configuration                       Set Parameters of Serial Port 7

iManager Chipset                  EIO-201
Firmware Version                  X00013608
OEM Group GPIO Number Available   0

▶ Serial Port 7 Configuration
▶ Serial Port 8 Configuration
▶ Hardware Monitor
▶ Watch Dog Timer Configuration

▶ ACPI Report Method Configuration           →←: Select Screen
▶ Digital I/O Configuration                  ↑↓: Select Item
                                             Enter: Select
                                             +/-: Change Opt.
                                             F1: General Help
                                             F2: Previous Values
                                             F3: Optimized Defaults
                                             F4: Save & Exit
                                             ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

- **Serial Port 7 Configuration**
  Set Parameters of Serial Port 7.
- **Serial Port 8 Configuration**
  Set Parameters of Serial Port.

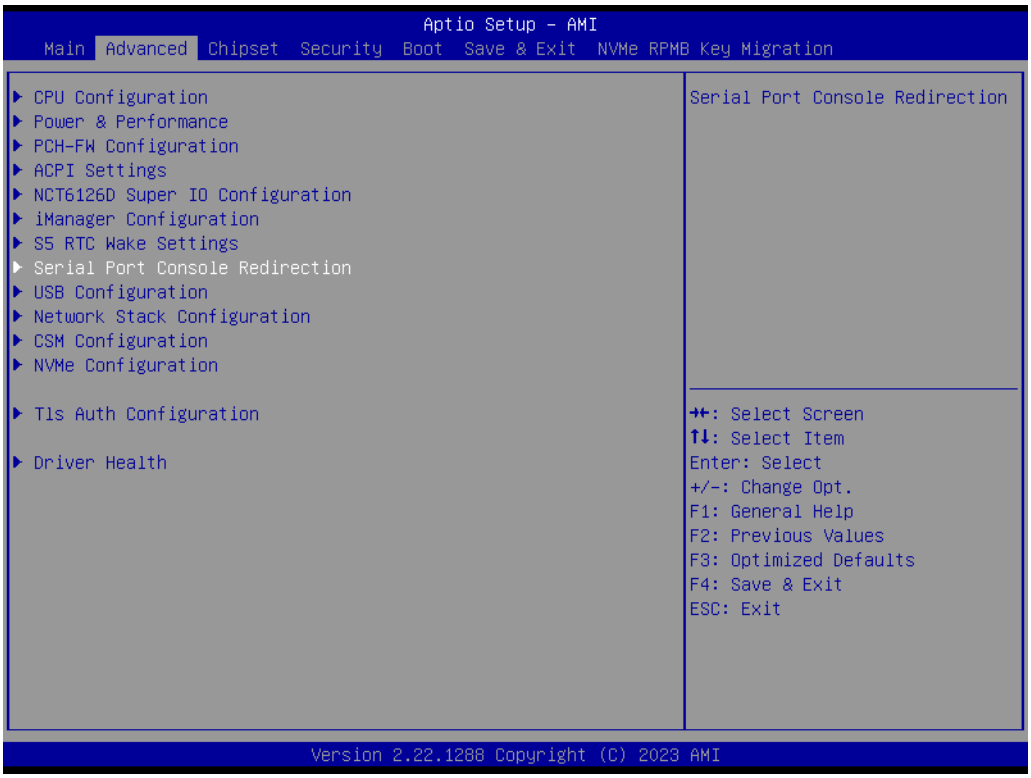
- **Hardware Monitor**
  Monitor hardware status.
- **Watch Dog Timer Configuration**
  Watch Dog Timer Configuration page.
- **ACPI Report Method Configuration**
  Select ACPI Reporting Method for EC Devices.
- **Digital I/O Configuration**
  Configure the digital I/O pins.

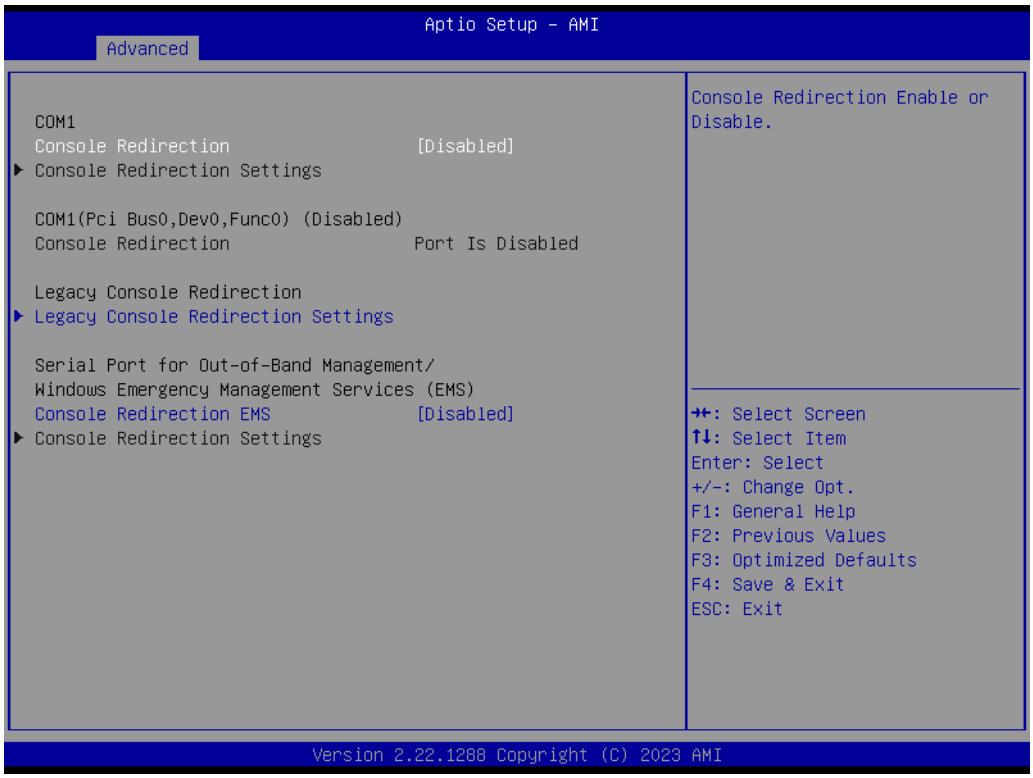
3.2.2.7 S5 RTC Wake Settings



- **Wake system from S5**
  Enable or disable system wake on alarm event.

3.2.2.8 Serial Port Console Redirection





- **Console Redirection**
  Console Redirection Enable or Disable.
- **Legacy Console Redirection Settings**
  Legacy Console Redirection Settings.
- **Console Redirection EMS**
  Console Redirection Enable or Disable.

3.2.2.9 USB Configuration

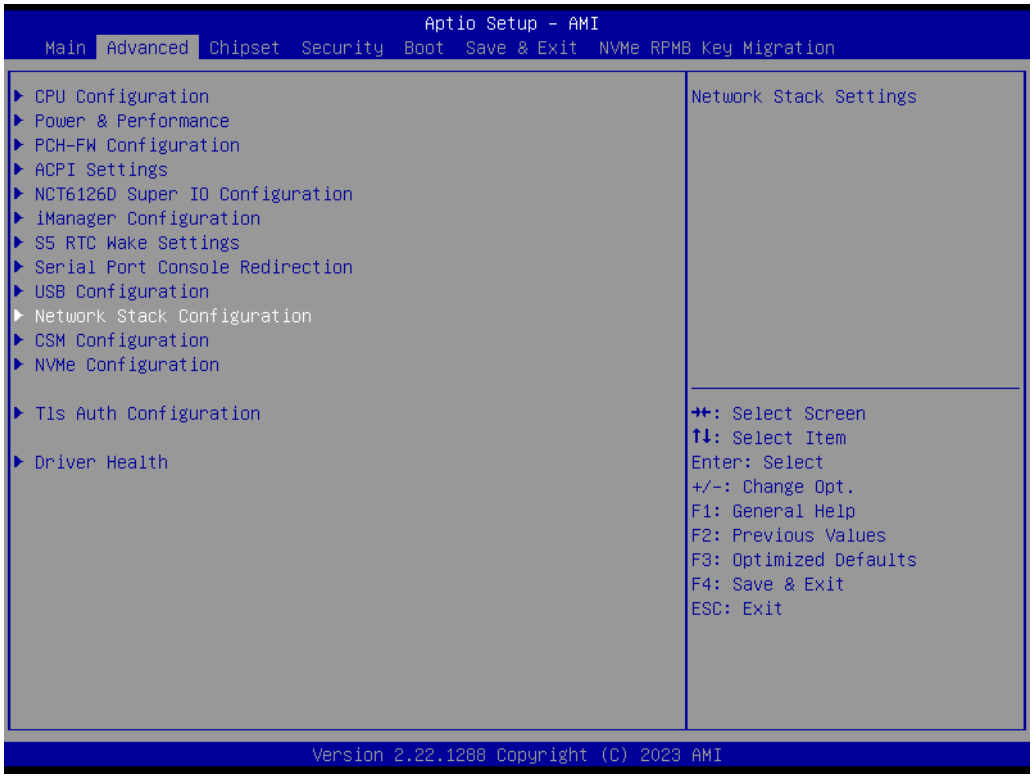
```
Aptio Setup - AMI
Main  Advanced  Chipset  Security  Boot  Save & Exit  NVMe RPMB Key Migration

▶ CPU Configuration                          USB Configuration Parameters
▶ Power & Performance
▶ PCH-FW Configuration
▶ ACPI Settings
▶ NCT6126D Super IO Configuration
▶ iManager Configuration
▶ S5 RTC Wake Settings
▶ Serial Port Console Redirection
▶ USB Configuration
▶ Network Stack Configuration
▶ CSM Configuration
▶ NVMe Configuration

▶ Tls Auth Configuration                     →←: Select Screen
                                             ↑↓: Select Item
▶ Driver Health                              Enter: Select
                                             +/-: Change Opt.
                                             F1: General Help
                                             F2: Previous Values
                                             F3: Optimized Defaults
                                             F4: Save & Exit
                                             ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

```
Aptio Setup - AMI
Advanced

USB Configuration                            Enables Legacy USB support.
                                             AUTO option disables legacy
USB Module Version              31           support if no USB devices are
                                             connected. DISABLE option will
USB Controllers:                             keep USB devices available
      2 XHCIs                                only for EFI applications.
USB Devices:
      1 Drive, 1 Keyboard, 1 Mouse, 1 Hub

Legacy USB Support              [Enabled]
XHCI Hand-off                   [Enabled]
USB Mass Storage Driver Support [Enabled]

USB hardware delays and time-outs:           →←: Select Screen
USB transfer time-out           [20 sec]     ↑↓: Select Item
Device reset time-out           [20 sec]     Enter: Select
Device power-up delay           [Auto]       +/-: Change Opt.
                                             F1: General Help
Mass Storage Devices:                        F2: Previous Values
JetFlashTS4GJFV30 8.07          [Auto]       F3: Optimized Defaults
                                             F4: Save & Exit
                                             ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

- **Legacy USB Support**
  Enables Legacy USB support.
- **XHCI Hand-off**
  This is a workaround for OS without XHCI hand-off support.

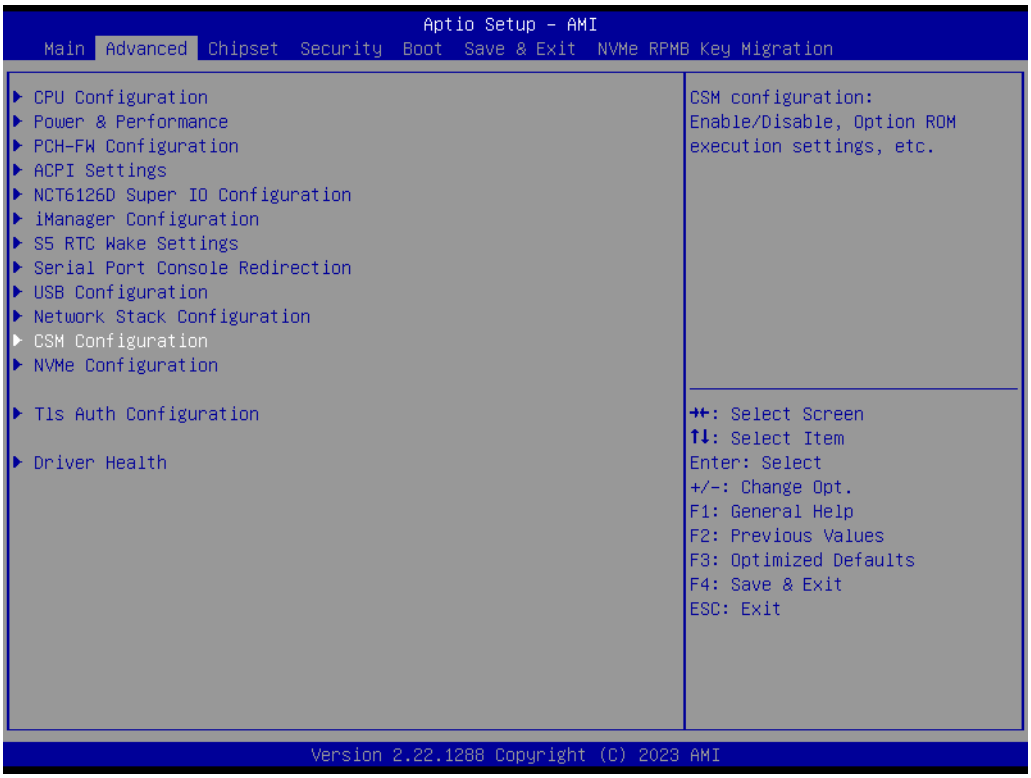
- **USB Mass Storage Device Configuration**
  Configure the USB Mass Storage Devices.
- **USB transfer time-out**
  The time-out value for Control, Bulk, and Interrupt transfers.
- **Device reset time-out**
  USB mass storage device Start Unit command time-out.
- **Device power-up delay**
  Maximum time the device will take before it properly reports itself to the Host Controller.

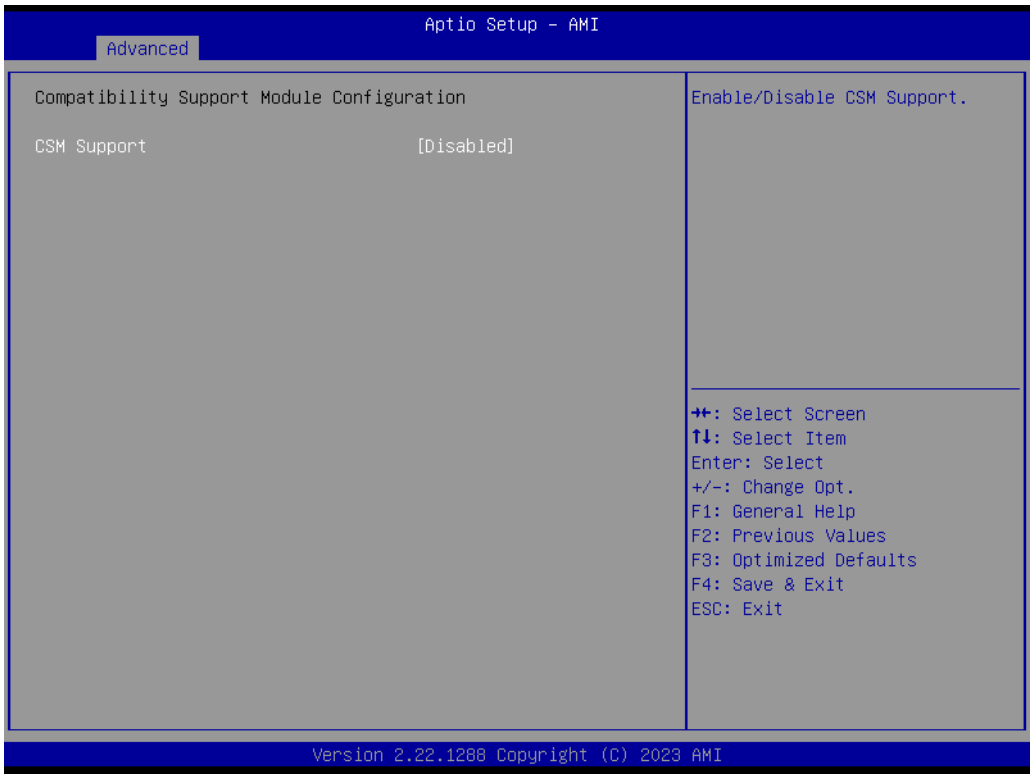
3.2.2.10 Network Stack Configuration



- **Network Stack**
  Enable/Disable UEFI Network Stack.

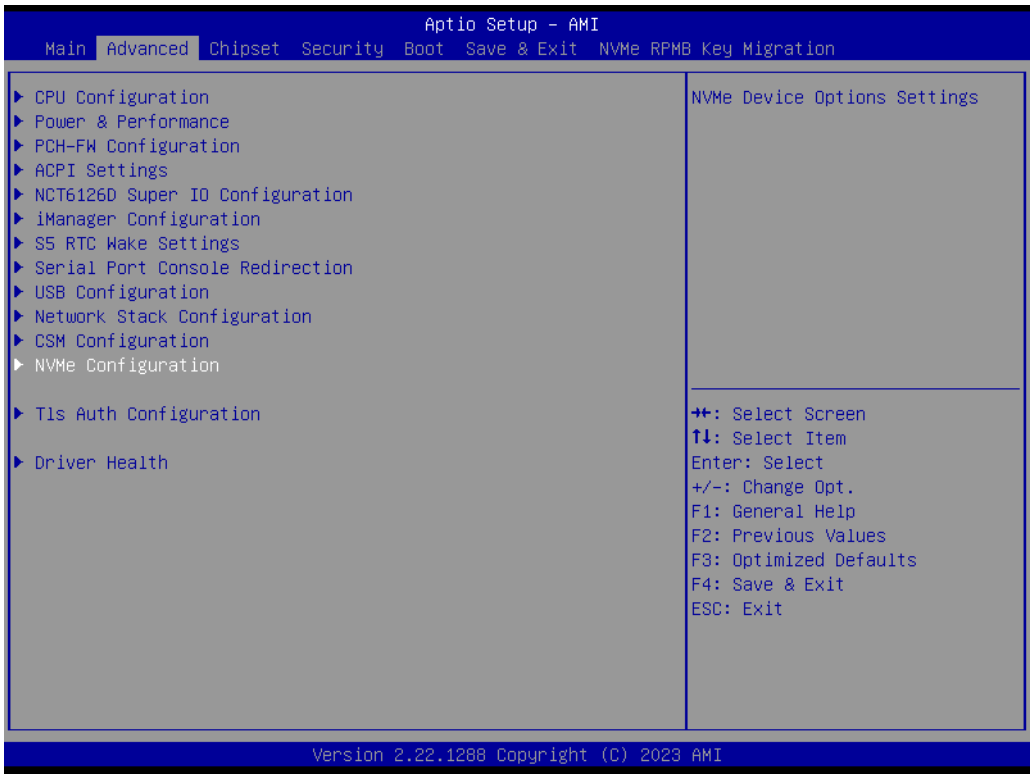
3.2.2.11 CSM Configuration

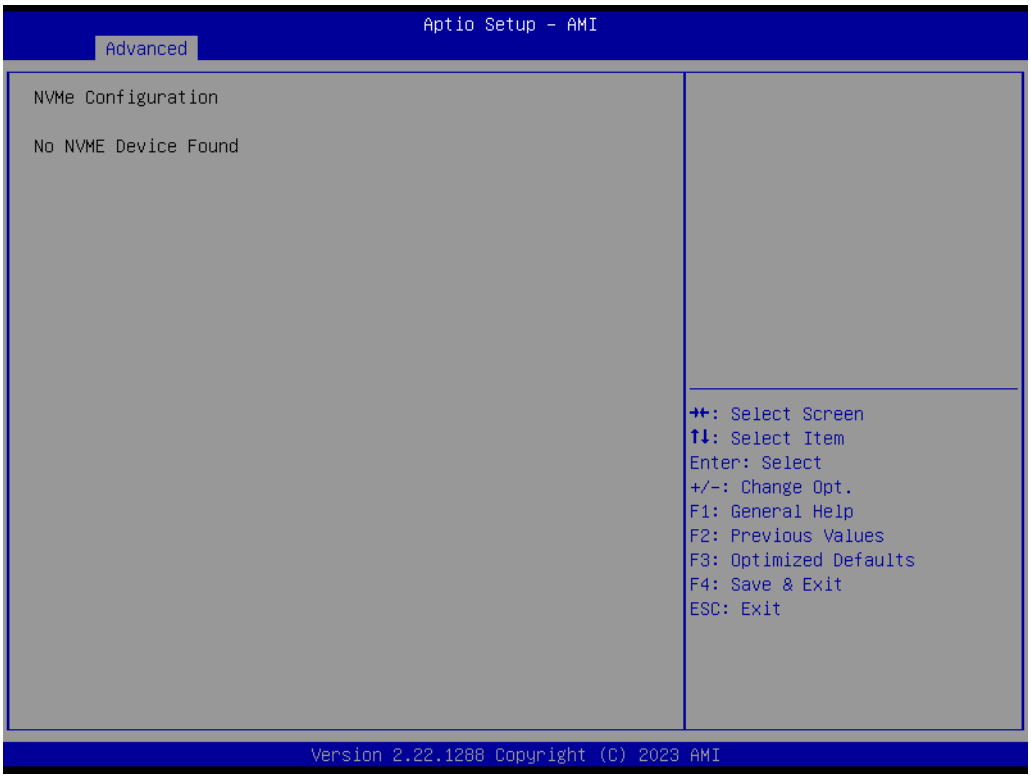




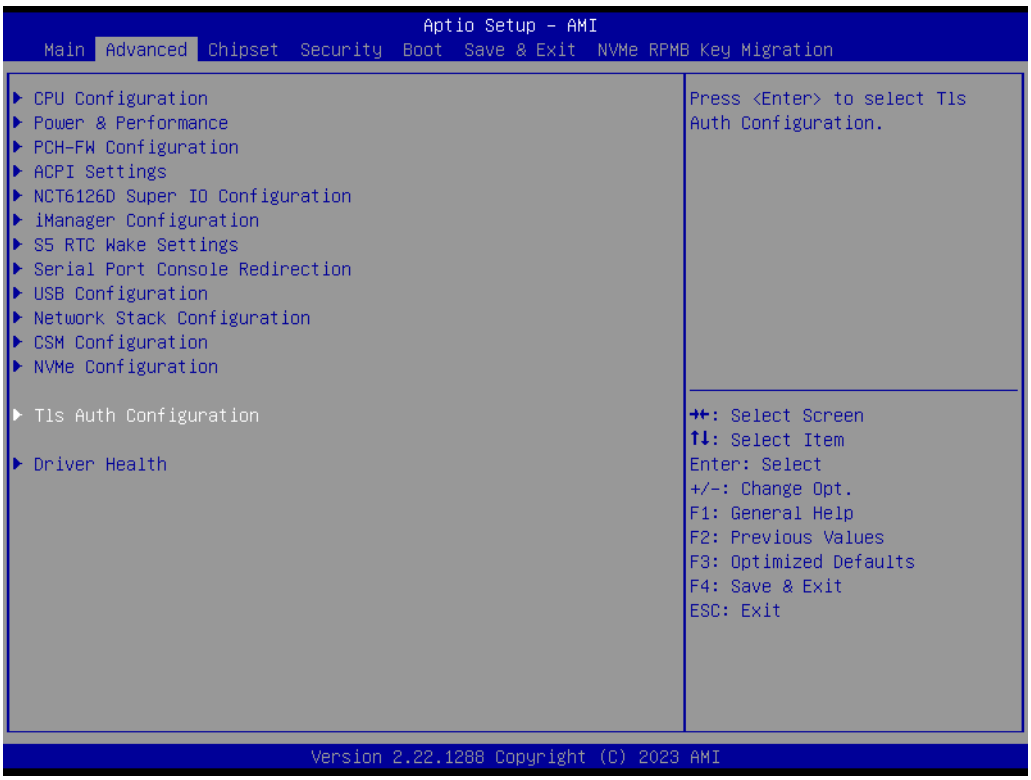
- **CSM Support**
  Enable/Disable CSM Support.

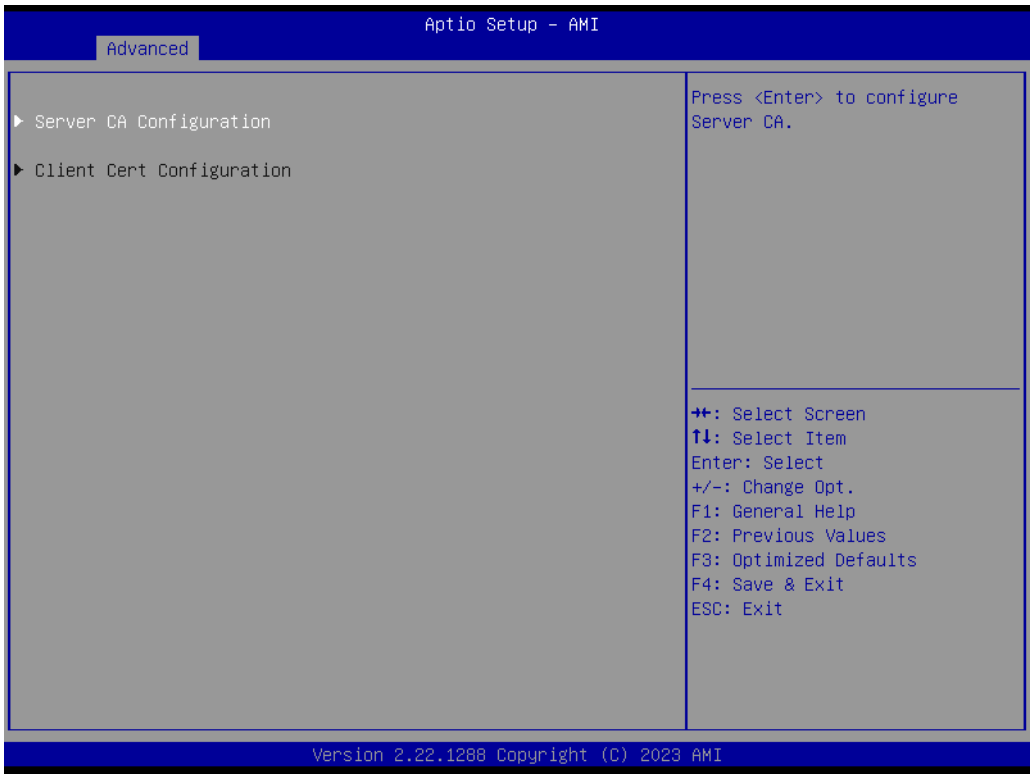
3.2.2.12 NVMe Configuration





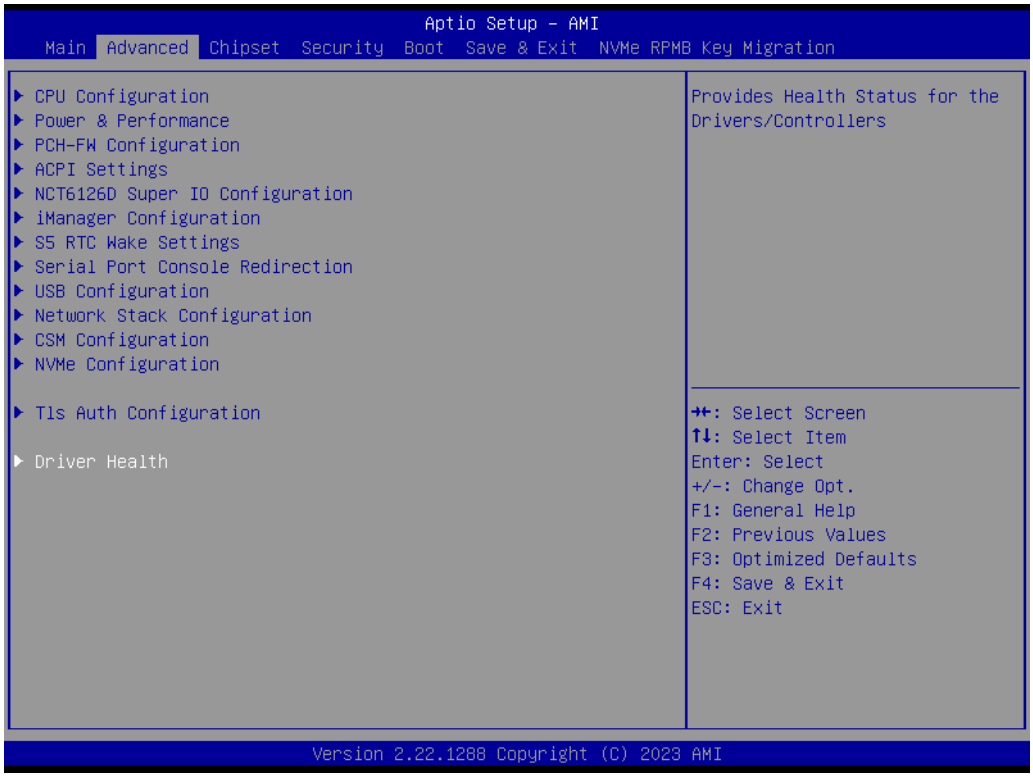
3.2.2.13 Tls Auth Configuration

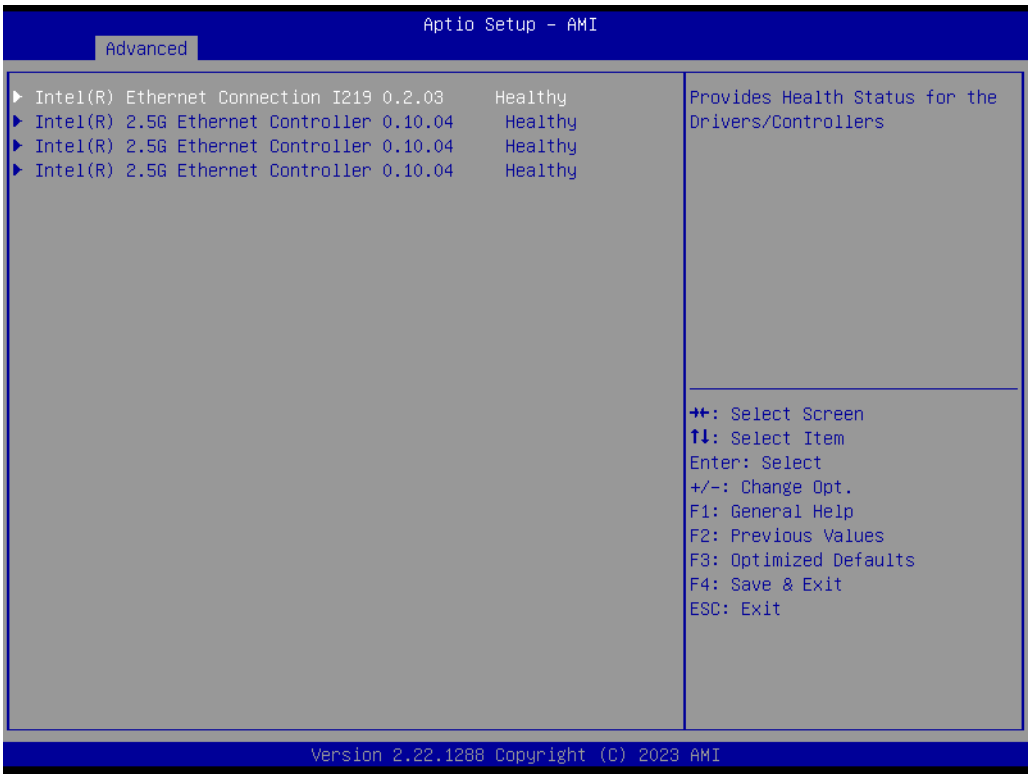




- **Sever CA Configuration**
  Press <Enter> to configure Server CA.
- **Client Cert Configuration**
  Client cert configuration is unsupported currently.

3.2.2.14 Driver Health





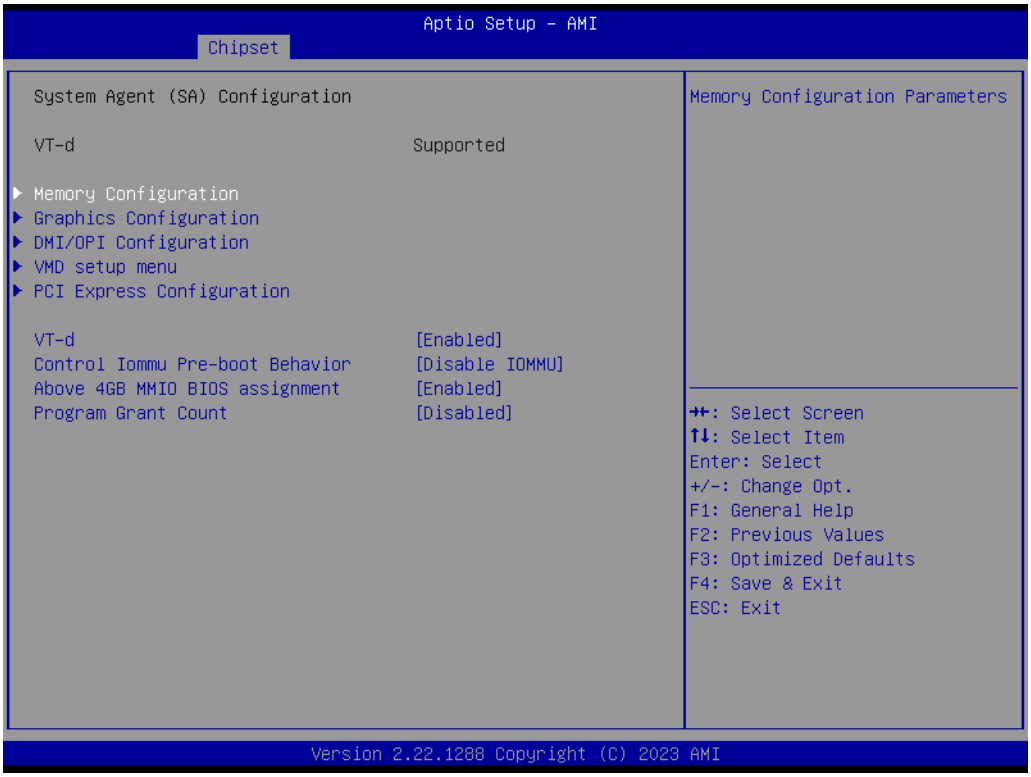
- **Provides Health Status for the Drivers/Controllers**

3.2.3 Chipset Configuration

Select the Chipset tab from the ARK-3533 setup screen to enter the Chipset BIOS Setup screen. You can display a Chipset BIOS Setup option by highlighting it using the <Arrow> keys. All Plug-and-Play BIOS Setup options are described in this section. The Plug-and-Play BIOS Setup screen is shown below.

3.2.3.1 System Agent Configuration

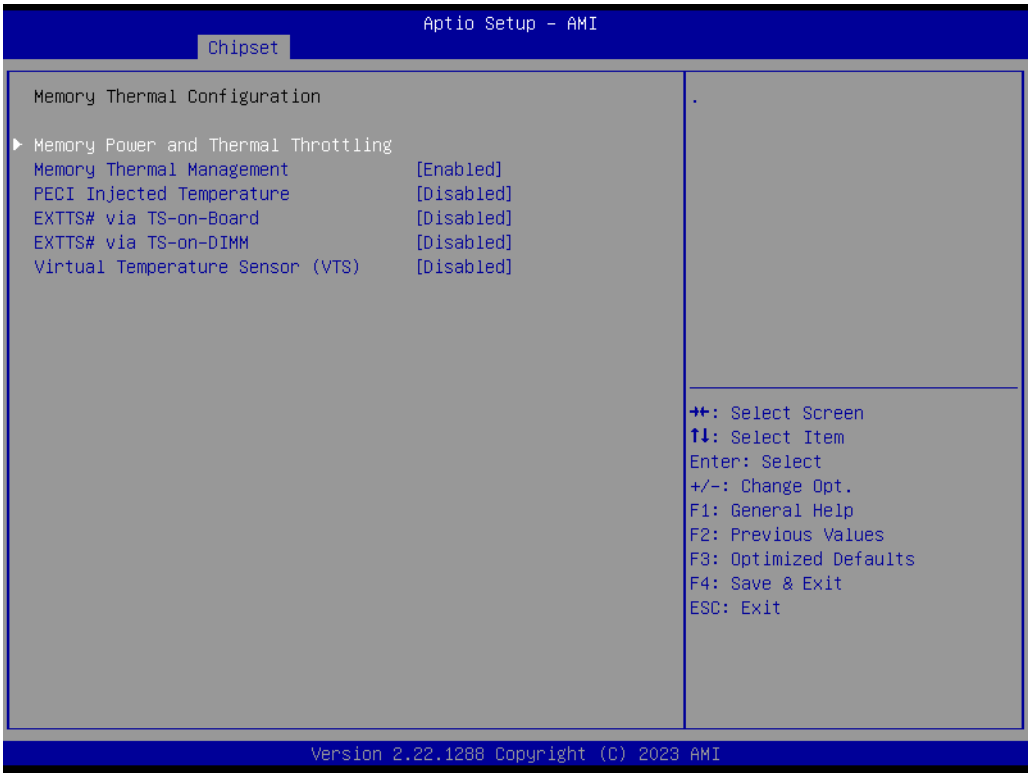
Memory Configuration Options



- **VT-d**
  VT-d capability.
- **Control Iommu Pre-boot Behavior**
- **Above 4GB MMIO BIOS assignment**
  Enable/Disable above 4GB Memory Mapped I/O BIOS assignment. This is enabled automatically when Aperture Size is set to 2048MB.

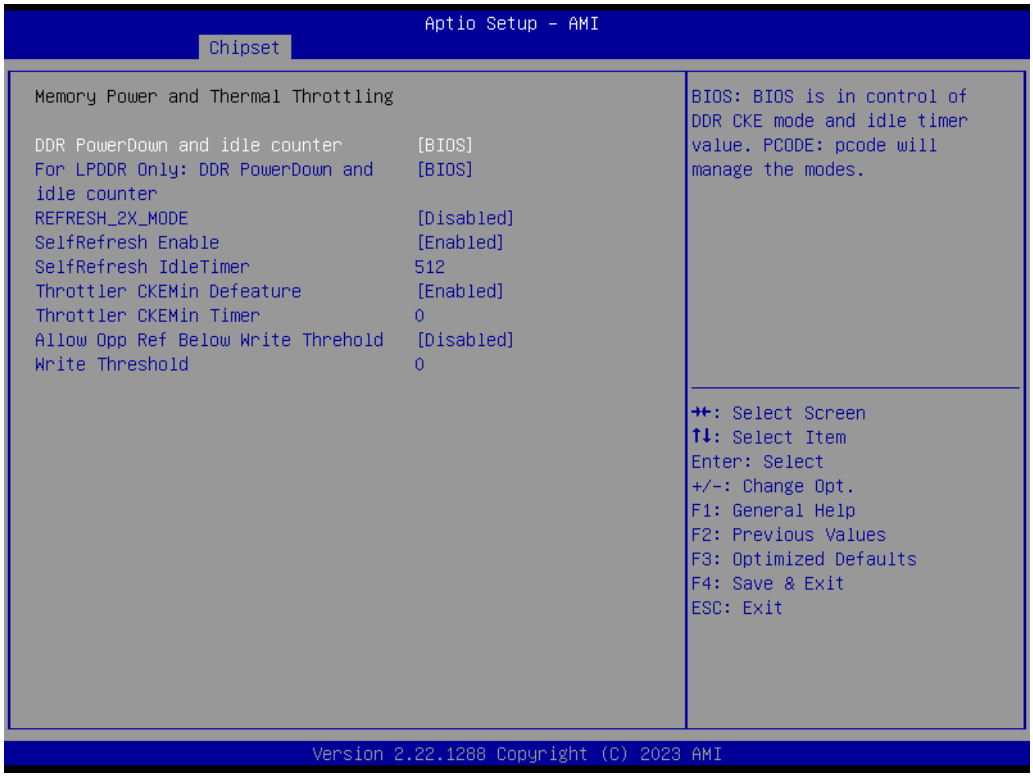
– **SAM Overloading**
  Enable/Disable SAM Overloading.

Memory Thermal Configuration



- **Memory Thermal Management**
  Enable/Disable Memory Thermal Management.
- **PECI Injected Temperature**
  Enable/Disable memory temperatures to be injected to the processor via PECI.
- **EXTTS# via TS-on-Board**
  Enable/Disable routing TS-on-Board's ALERT# and THERM# to EXTTS# pins on the PCH.
- **EXTTS# via TS-on-DIMM**
  Enable/Disable routing TS-on-DIMM ALERT# to EXTTS# pin on the PCH.
- **Virtual Temperature Sensor (VTS)**
  Enable/Disable Virtual Temperature Sensor (VTS).

Memory Power and Thermal Throttling



- **DDR PowerDown and idle counter**
  BIOS: BIOS is in control of DDR CKE mode and idle timer value. PCODE: pcode will manage the modes.
- **For LPDDR only: DDR PowerDown and idle counter**
  For LPDDR Only: BIOS: BIOS is in control of DDR CKE mode and idle timer value. PCODE: pcode will manage the modes.
- **REFRESH_2X_MODE**
  0- Disabled 1-iMC enables 2xRef when Warm and Hot 2- iMC enables 2xRef when Hot.
- **SelfRefresh Enable**
  Enable, Disable(Enable= Def)
- **SelfRefresh IdleTimer**
  Range [64K-1;512]in DLCK800s, (512= Def)
- **Throttler CKEMin Defeature**
  On, Off.
- **Throttler CKEMin Timer**
  Timer value for CKEMin, range[255;0]. Req'd min of SC_ROUND_T + BYTE_LENGTH (4).
- **Allow Opp Ref Below Write Threshold**
  Allow opportunistic refreshes while we don't exit power down.
- **Write Threshold**
  Number of writes that can be accumulated while CKE is low before CKE is asserted.

Graphics Configuration

```
Aptio Setup - AMI
Chipset

System Agent (SA) Configuration                    Graphics Configuration

VT-d                                Supported

▶ Memory Configuration
▶ Graphics Configuration
▶ DMI/OPI Configuration
▶ VMD setup menu
▶ PCI Express Configuration

VT-d                                [Enabled]
Control Iommu Pre-boot Behavior     [Disable IOMMU]
Above 4GB MMIO BIOS assignment      [Enabled]
Program Grant Count                 [Disabled]

                                    →←: Select Screen
                                    ↑↓: Select Item
                                    Enter: Select
                                    +/-: Change Opt.
                                    F1: General Help
                                    F2: Previous Values
                                    F3: Optimized Defaults
                                    F4: Save & Exit
                                    ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

```
Aptio Setup - AMI
Chipset

Graphics Configuration                             Graphics turbo IMON current
                                                   values supported (14-31)
Graphics Turbo IMON Current         31
Skip Scaning of External Gfx Card   [Disabled]

Primary Display                     [Auto]
▶ External Gfx Card Primary Display Configuration
Internal Graphics                   [Enabled]
GTT Size                            [8MB]
Aperture Size                       [256MB]
DVMT Pre-Allocated                  [60M]
DVMT Total Gfx Mem                  [256M]
Intel Graphics Pei Display Peim     [Disabled]
VDD Enable                          [Enabled]
Configure GT for use                [Enabled]
RC1p Support                        [Disabled]
PAVP Enable                         [Enabled]
Cdynmax Clamping Enable             [Disabled]
Cd Clock Frequency                  [Max CdClock freq
                                    based on Reference Clk]
                                    →←: Select Screen
                                    ↑↓: Select Item
                                    Enter: Select
                                    +/-: Change Opt.
                                    F1: General Help
                                    F2: Previous Values
                                    F3: Optimized Defaults
                                    F4: Save & Exit
                                    ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

- **Graphics Turbo IMON current**
  Graphics turbo IMON current values supported (14-31).
- **Skip Scanning of External Gfx Card**
  If Enabled, it will not scan for External Gfx Card on PEG and PCH PCIE Ports.

- **Primary Display**
  Select from IGFX/PEG/PCI, which graphics device should be Primary Display or select SG for Switchable Gfx.
- **External Gfx Card Primary Display Configuration**
  Select the card used on the platform.
- **Internal Graphics**
  Keep IGFX enabled based on the setup options.
- **GTT Size**
  Select the GTT Size.
- **Aperture Size**
  Select the Aperture Size.
- **PSMI SUPPORT**
  PSMI Enable/Disable.
  DVMT Pre-Allocated
  Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.
- **Intel Graphics Pei Display Peim**
  Enable/Disable Pei (Early) Display.
- **VDD Enable**
  Enable/Disable forcing of VDD in the BIOS.
- **Configure GT for use**
  Enable/Disable GT configuration in BIOS.
- **RC1p Support**
  Enable/Disable RC1p support. If RC1p is enabled, send a RC1p frequency request to PMA based other conditions being met.
- **PAVP Enable**
  Enable/Disable PAVP.
- **Cdynmax Clamping Enable**
  Enable/Disable Cdynmax Clamping.
- **Cd Clock Frequency**
  Select the highest Cd Clock frequency supported by the platform.

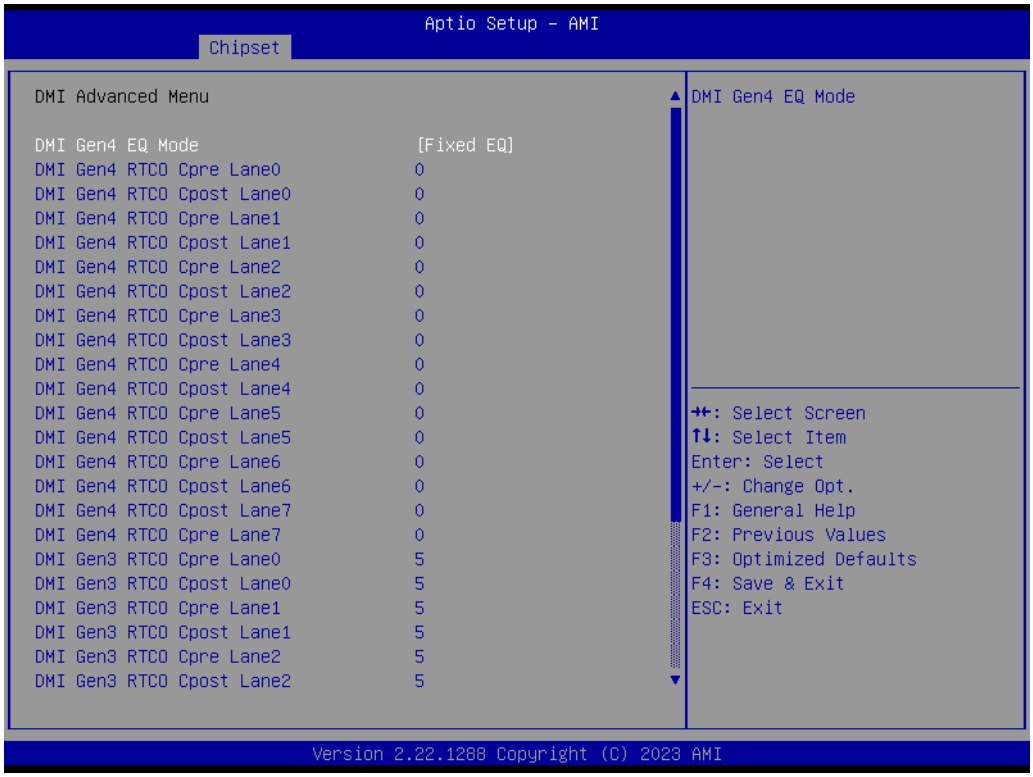
DMI/OPI Configuration

```
Aptio Setup - AMI
Chipset

System Agent (SA) Configuration                    Control various DMI functions.

VT-d                                Supported

▶ Memory Configuration
▶ Graphics Configuration
▶ DMI/OPI Configuration
▶ VMD setup menu
▶ PCI Express Configuration

VT-d                                [Enabled]
Control Iommu Pre-boot Behavior     [Disable IOMMU]
Above 4GB MMIO BIOS assignment      [Enabled]
Program Grant Count                 [Disabled]

                                    →←: Select Screen
                                    ↑↓: Select Item
                                    Enter: Select
                                    +/-: Change Opt.
                                    F1: General Help
                                    F2: Previous Values
                                    F3: Optimized Defaults
                                    F4: Save & Exit
                                    ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

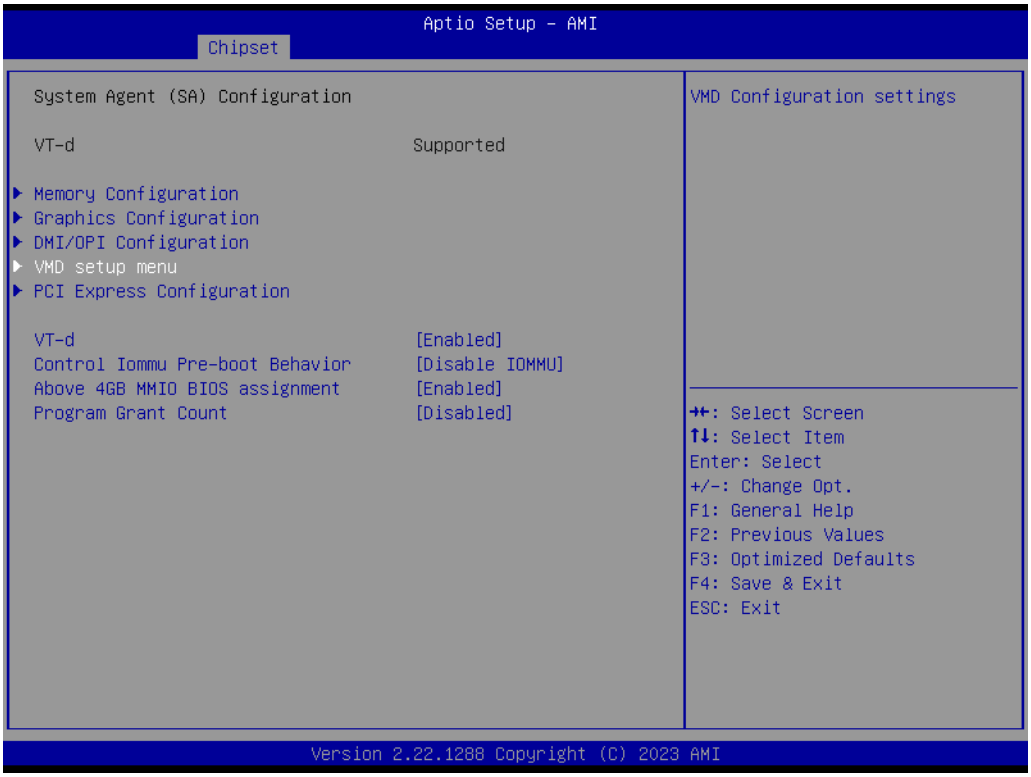
```
Aptio Setup - AMI
Chipset

DMI/OPI Configuration                              Set DMI Speed Gen1/Gen2/Gen3

DMI                                 X4  Gen4

DMI Max Link Speed                  [Gen4]
CDR Relock for CPU DMI              [Disabled]
DMI ASPM                            [ASPM L1]
DMI Gen3 L1 Exit Latency            4
New FOM for CPU DMI                 [Disabled]
▶ DMI Advanced Menu

                                    →←: Select Screen
                                    ↑↓: Select Item
                                    Enter: Select
                                    +/-: Change Opt.
                                    F1: General Help
                                    F2: Previous Values
                                    F3: Optimized Defaults
                                    F4: Save & Exit
                                    ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

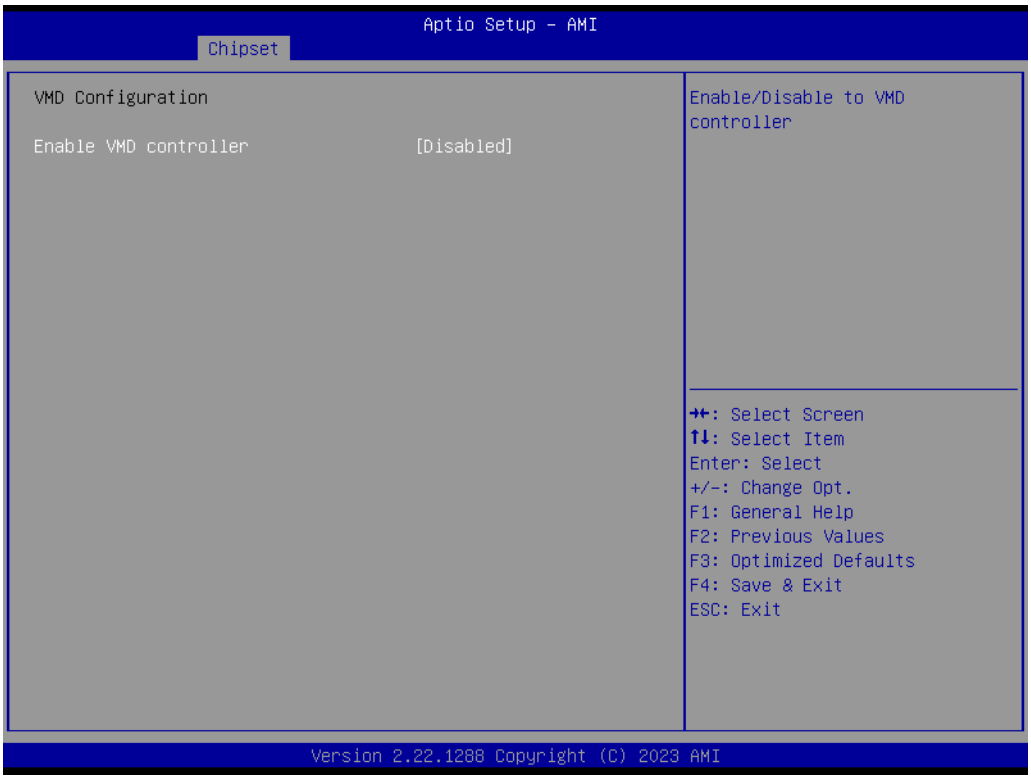
- **DMI Max Link Speed**
  Set DMI Speed Gen1/Gen2/Gen3.
- **CDR Relock for CPU DMI**
  Enable/Disable CDR Relock.

– **DMI ASPM**
  DMI ASPM Support.
– **DMI Gen3 L1 Latency**
  DMI Gen3 L1 Exit Latency.
– **New FOM for CPU DMI**
  Enable/Disable New FOM.



VMD Setup Menu





– **Enable VMD Controller**
  Enable/Disable to VMD controller.

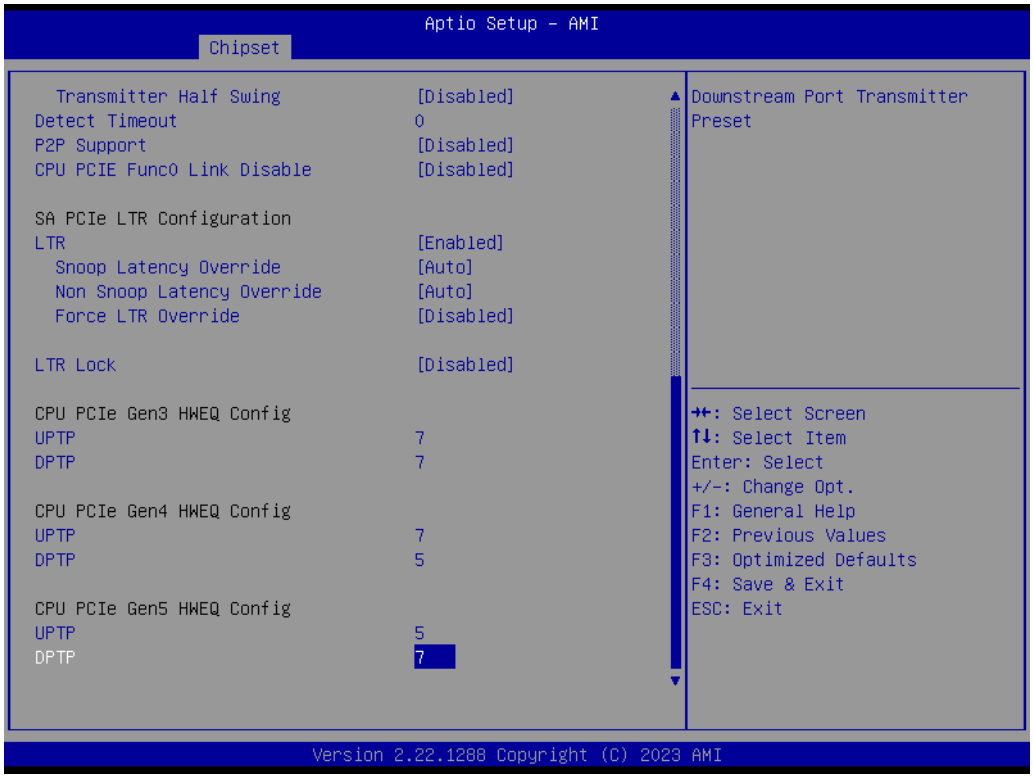
MXM 3.1 (3D) Controller

```
Aptio Setup - AMI
Chipset

System Agent (SA) Configuration                    PCI Express Configuration
                                                   settings
VT-d                                Supported

▶ Memory Configuration
▶ Graphics Configuration
▶ DMI/OPI Configuration
▶ VMD setup menu
▶ PCI Express Configuration

VT-d                                [Enabled]
Control Iommu Pre-boot Behavior     [Disable IOMMU]
Above 4GB MMIO BIOS assignment      [Enabled]
Program Grant Count                 [Disabled]

                                                   →←: Select Screen
                                                   ↑↓: Select Item
                                                   Enter: Select
                                                   +/-: Change Opt.
                                                   F1: General Help
                                                   F2: Previous Values
                                                   F3: Optimized Defaults
                                                   F4: Save & Exit
                                                   ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

```
Aptio Setup - AMI
Chipset

PCI Express Configuration                          PCI Express Root Port Settings.

▶ MXM 3.1 (3D) Controller
▶ CPU PCI Express Root Port 3

                                                   →←: Select Screen
                                                   ↑↓: Select Item
                                                   Enter: Select
                                                   +/-: Change Opt.
                                                   F1: General Help
                                                   F2: Previous Values
                                                   F3: Optimized Defaults
                                                   F4: Save & Exit
                                                   ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

- **PCI Express Clock Gating**
  PCI Express Clock Gating Enable/Disable for each root port.
- **PCI Express Power Gating**
  PCI Express Power Gating Enable/Disable for each root port.
- **ASPM**
  PCI Express Active State Power Management settings.
- **L1 Substates**
  PCI Express L1 Substates settings. L1SS cannot be enabled when CLKREQMSG is disabled.
- **Gen3 EQ Phase3 Method**
  PCIe Gen3 Equalization Phase 3 Method.
- **Gen4 EQ Phase3 Method**
  PCIe Gen4 Equalization Phase 3 Method.
- **ACS**
  Enable/Disable Access Control Services Extended Capability.
- **PTM**
  Enable/Disable Precision Time Measurement
- **DPC**
  Enable/Disable Downstream Port Containment
- **FOM Scoreboard Control Policy**
  Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS.
- **Multi-VC**
  Enable/Disable Multi Virtual Channel.
- **EDPC**
  Enable/Disable Rootport extensions for Downstream Port Containment.
- **URR**
  PCI Express Unsupported Request Reporting Enable/Disable.

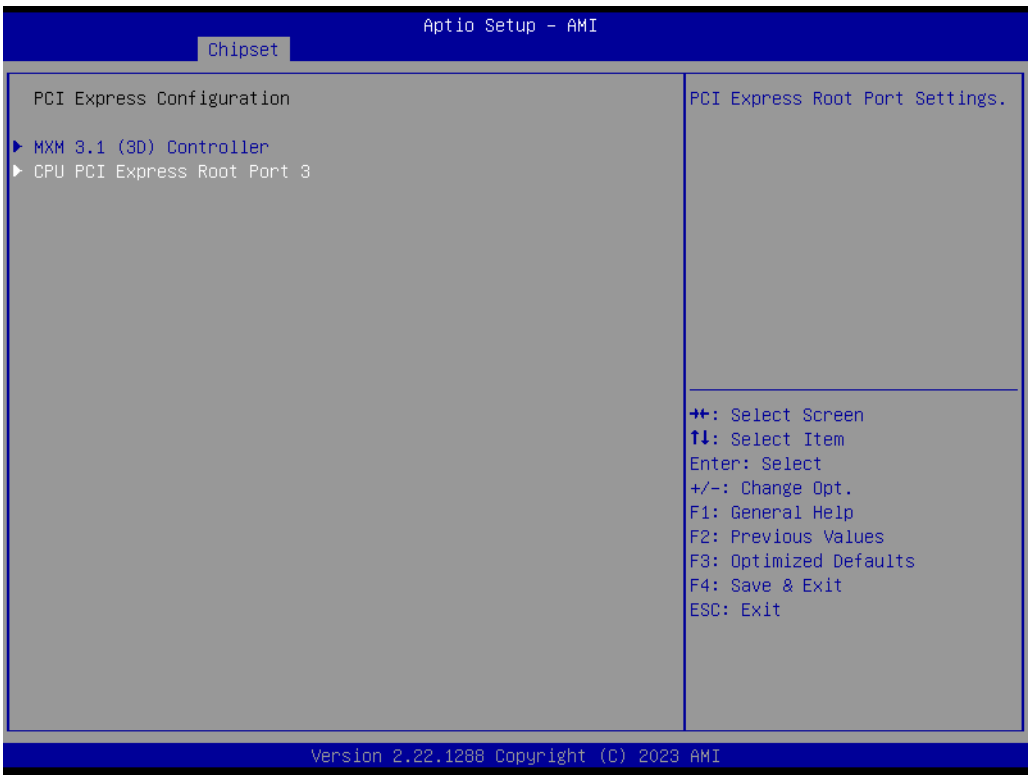
- **FER**
  PCI Express Device Fatal Error Reporting Enable/Disable.
- **NFER**
  PCI Express Device Non-Fatal Error Reporting Enable/Disable.
- **CER**
  PCI Express Device Correctable Error Reporting Enable/Disable.
- **CTO**
  PCI Express Device Correctable Error Reporting Enable/Disable.
- **SEFE**
  Root PCI Express System Error on Fatal Error Enable/Disable.
- **SENFE**
  Root PCI Express System Error on Non-Fatal Error Enable/Disable.
- **SECE**
  Root PCI Express System Error on Correctable Error Enable/Disable.
- **PME SCI**
  PCI Express PME SCI Enable/Disable.
- **Advanced Error Reporting**
  Advanced Error Reporting Enable/Disable.
- **Cle Speed**
  Configure PCIe Speed.
- **Enable ClockReq Messaging**
  Enable or Disable ClockReq Messaging.



- **Transmitter Half Swing**
  Transmitter Half Swing Enable/Disable.
- **P2P Support**
  Program P2P Support Registers according to setup option.

- **CPU PCIe Func0 Link Disable**
  CPU PCIE Func0 Link Disable while Device attached into Port having Func0 and FuncN.
- **LTR**
  SA PCIE Latency Reporting Enable/Disable.
- **Snoop Latency Override**
  Snoop Latency Override for SA PCIE.
- **Non Snoop Latency Override**
  Non Snoop Latency Override for SA PCIE.
- **Force LTR Override**
  Force LTR Override for SA PCIE.
- **LTR Lock**
  PCIE LTR Configuration Lock.
- **UPTP**
  Upstream Port Transmitter Preset.
- **DPTP**
  Downstream Port Transmitter Preset.

CPU PCI Express Root Port 3



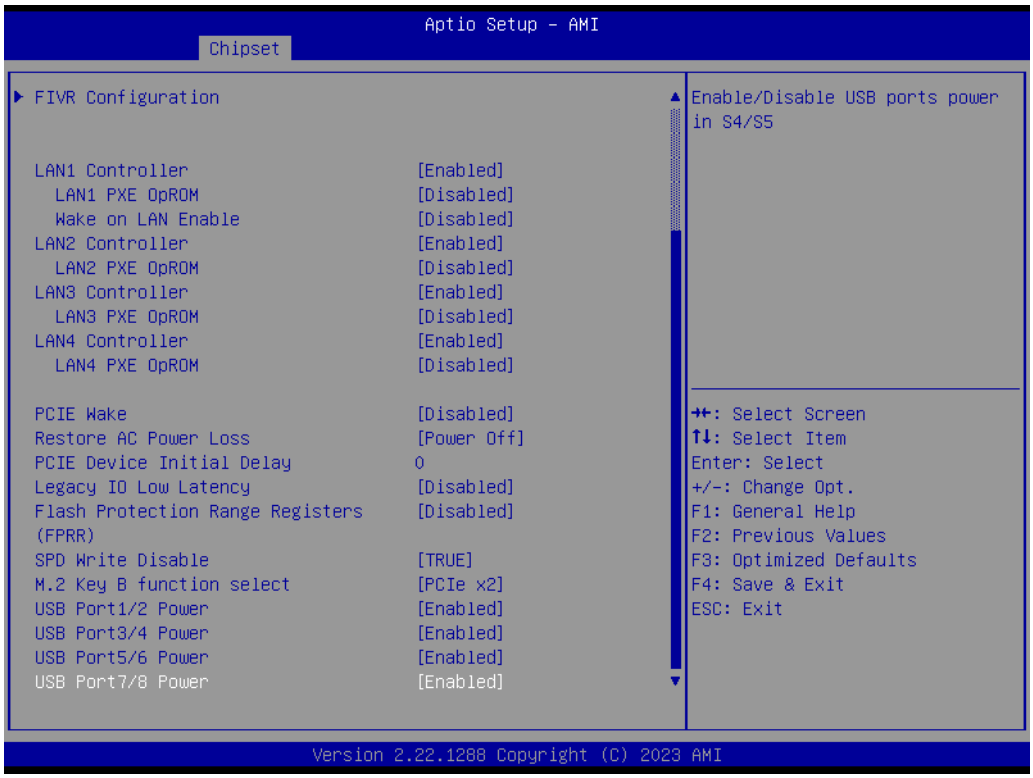
```
Aptio Setup - AMI
Chipset

Connection Type                    [Slot]
PCI Express Clock Gating           [Enabled]
PCI Express Power Gating           [Enabled]
ASPM                               [Disabled]
L1 Substates                       [Disabled]
Gen3 Eq Phase3 Method              [Hardware]
Gen4 Eq Phase3 Method              [Hardware]
ACS                                [Enabled]
PTM                                [Enabled]
DPC                                [Disabled]
FOM Scoreboard Control Policy      [Auto]
Multi-VC                           [Enabled]
EDPC                               [Enabled]
  URR                              [Enabled]
  FER                              [Enabled]
  NFER                             [Enabled]
  CER                              [Enabled]
  CTO                              [Disabled]
  SEFE                             [Disabled]
  SENFE                            [Disabled]
  SECE                             [Disabled]
  PME SCI                          [Enabled]
  Advanced Error Reporting         [Enabled]
PCIe Speed                         [Auto]
Enable ClockReq Messaging          [Disabled]

Built-In: a built-in device is
connected to this rootport.
SlotImplemented bit will be
clear. Slot: this rootport
connects to user-accessible
slot. SlotImplemented bit will
be set.

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

```
Aptio Setup - AMI
Chipset

Enable ClockReq Messaging          [Disabled]
  Transmitter Half Swing           [Disabled]
Detect Timeout                     0
P2P Support                        [Disabled]

SA PCIe LTR Configuration
LTR                                [Enabled]
  Snoop Latency Override           [Auto]
  Non Snoop Latency Override       [Auto]
  Force LTR Override               [Disabled]

LTR Lock                           [Disabled]

CPU PCIe Gen3 HWEQ Config
UPTP                               7
DPTP                               7

CPU PCIe Gen4 HWEQ Config
UPTP                               7
DPTP                               5

CPU PCIe Gen5 HWEQ Config
UPTP                               5
DPTP                               7

Downstream Port Transmitter
Preset

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

3.2.3.2 PCH-IO Configuration

```
Aptio Setup - AMI
Main  Advanced  Chipset  Security  Boot  Save & Exit  NVMe RPMB Key Migration

▶ System Agent (SA) Configuration
▶ PCH-IO Configuration

PCH Parameters

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

```
Aptio Setup - AMI
Chipset

PCH-IO Configuration

▶ PCI Express Configuration
▶ SATA Configuration
▶ USB Configuration
▶ Security Configuration
▶ HD Audio Configuration
▶ FIVR Configuration

LAN1 Controller                [Enabled]
  LAN1 PXE OpROM               [Disabled]
  Wake on LAN Enable           [Disabled]
LAN2 Controller                [Enabled]
  LAN2 PXE OpROM               [Disabled]
LAN3 Controller                [Enabled]
  LAN3 PXE OpROM               [Disabled]
LAN4 Controller                [Enabled]
  LAN4 PXE OpROM               [Disabled]

PCIE Wake                      [Disabled]
Restore AC Power Loss          [Power Off]
PCIE Device Initial Delay      0
Legacy IO Low Latency          [Disabled]

PCI Express Configuration
settings

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```



- **LAN1~4 Controller**
  Enable/Disable onboard NIC.
- **LAN1~4 PXE OpROM**
  Enable or disable boot option for LAN1 Controller.
- **Wake on LAN Enable**
  Enable/Disable integrated LAN to wake the system.
- **PCIE Wake**
  Enable or disable PCIE to wake the system from S5.
- **Restore AC Power Loss**
  Specify what state to go to when power is re-applied after a power failure (G3 state).
- **PCIE Device Initial Delay**
  The PCIE device initial delay 0~30 seconds.
- **Legacy IO Low Latency**
  Set to enable low latency of legacy IO. Some systems require lower IO latency irrespective of power. This is a tradeoff between power and IO latency.
- **Flash Protection Range Registers (FPRR)**
  Enable Flash Protection Range Registers.
- **SPD Write Disable**
  Enable/Disable setting SPD Write Disable. For security recommendations, SPD write disable bit must be set.
- **M.2 Key B function select**
  M.2 Key B function select.
- **USB Port Power**
  Enable/Disable USB ports power in S4/S5.

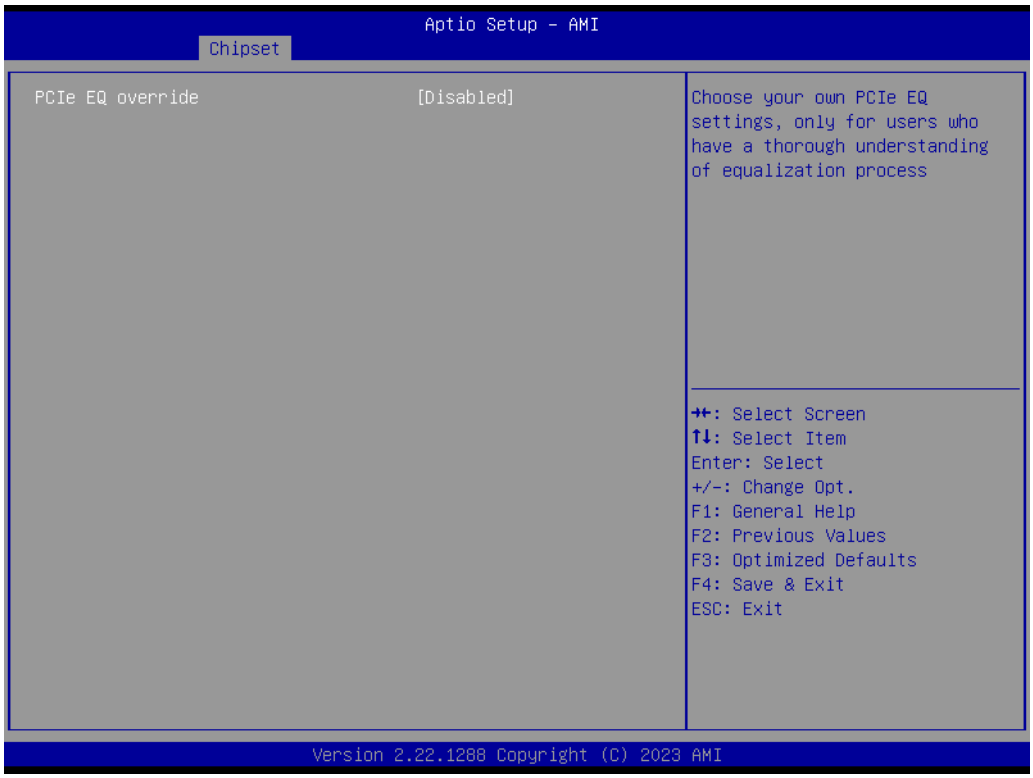
PCI Express Configuration

```
Aptio Setup - AMI
Chipset

PCH-IO Configuration

▶ PCI Express Configuration
▶ SATA Configuration
▶ USB Configuration
▶ Security Configuration
▶ HD Audio Configuration
▶ FIVR Configuration

LAN1 Controller                    [Enabled]
  LAN1 PXE OpROM                   [Disabled]
  Wake on LAN Enable               [Disabled]
LAN2 Controller                    [Enabled]
  LAN2 PXE OpROM                   [Disabled]
LAN3 Controller                    [Enabled]
  LAN3 PXE OpROM                   [Disabled]
LAN4 Controller                    [Enabled]
  LAN4 PXE OpROM                   [Disabled]

PCIE Wake                          [Disabled]
Restore AC Power Loss              [Power Off]
PCIE Device Initial Delay          0
Legacy IO Low Latency              [Disabled]

PCI Express Configuration
settings

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

– **DMI Link ASPM Control**
  The control of Active State Power Management of the DMI Link.

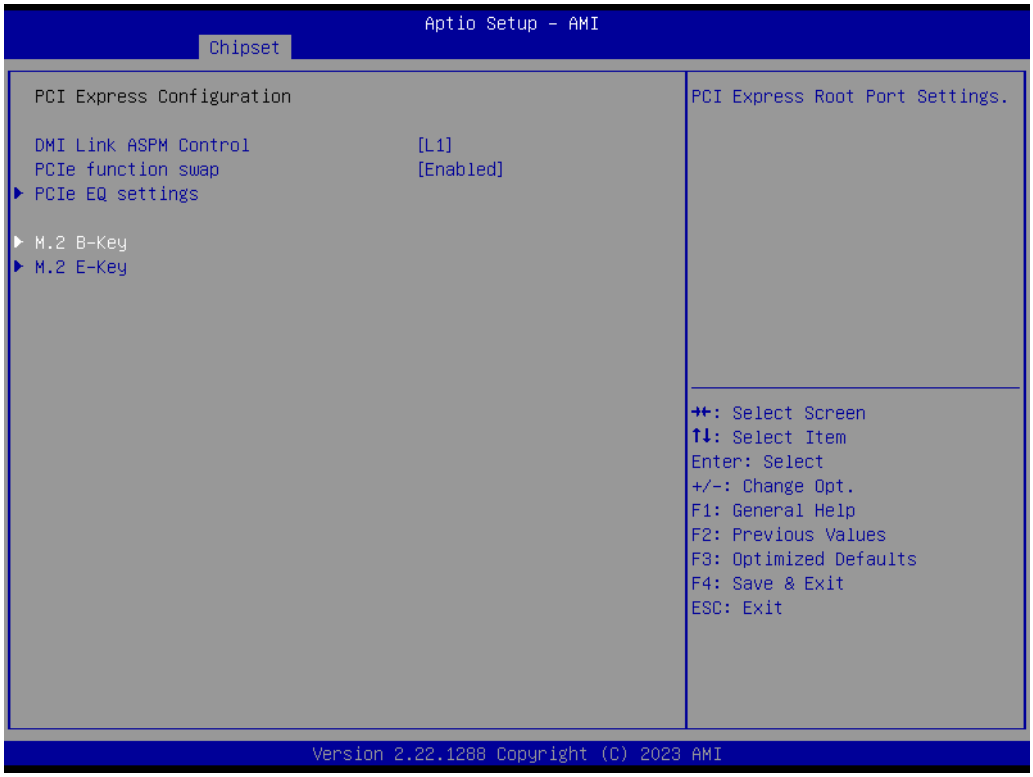
– **PCIe function swap**
  Enable/Disable PCIe function swap.

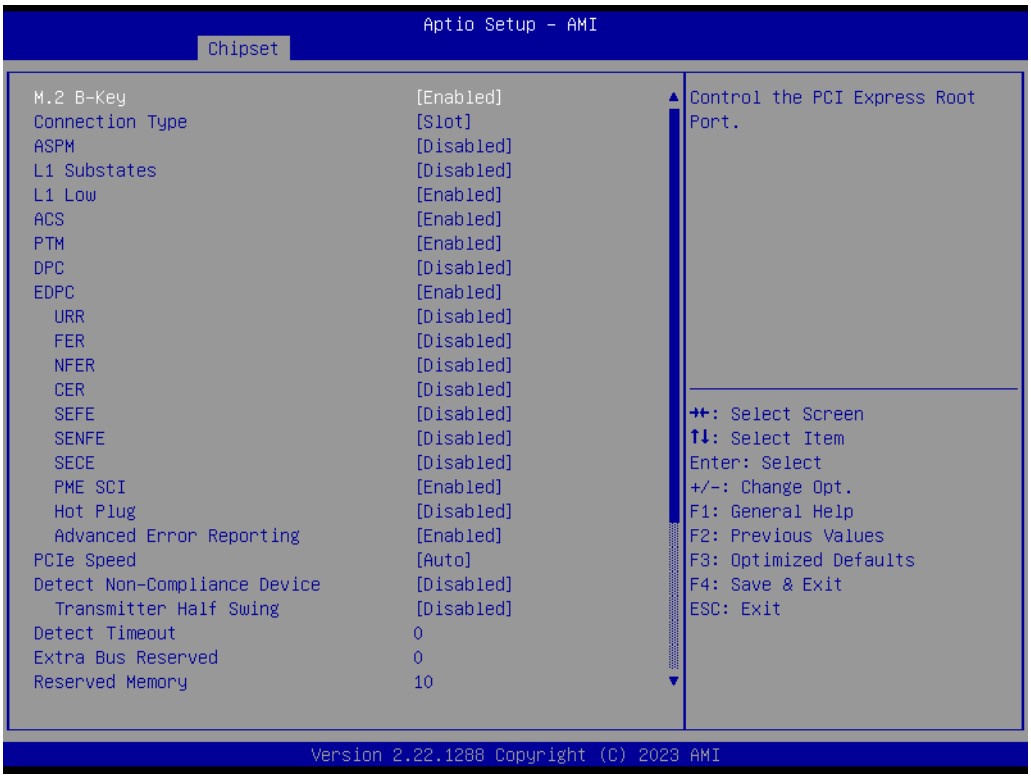
```
Aptio Setup - AMI
Chipset

PCI Express Configuration

DMI Link ASPM Control              [L1]
PCIe function swap                 [Enabled]
▶ PCIe EQ settings

▶ M.2 B-Key
▶ M.2 E-Key

This form contains options for
controlling PCIe EQ process

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

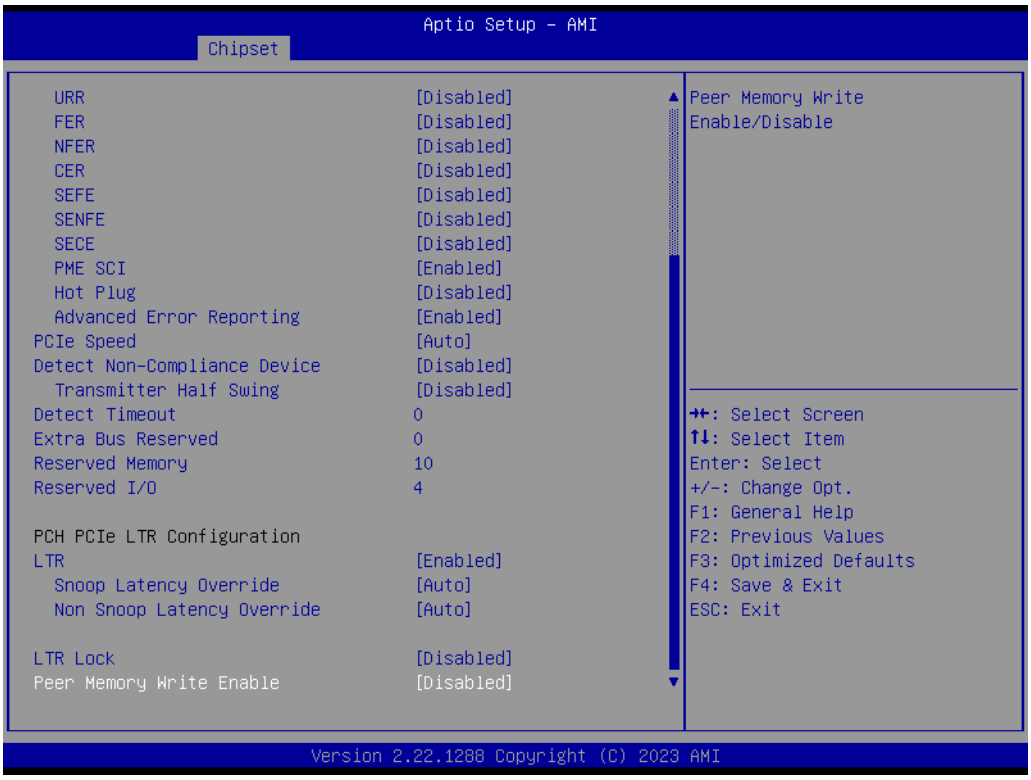


– **PCIe EQ override**
Choose your own PCIe EQ settings, only for users who have a thorough understanding of the equalization process.

M.2 B-Key







– **ASPM**
  PCI Express Active State Power Management settings.
– **L1 Substates**
  PCI Express L1 Substates settings.L1SS cannot be enabled when CLKREQMSG is disabled.

- **L1 Low**
  PCI Express L1 Low Substate Enable/Disable.
- **ACS**
  Enable/Disable Access Control Services Extended Capability.
- **PTM**
  Enable/Disable Precision Time Measurement.
- **DPC**
  Enable/Disable Downstream Port Containment.
- **EDPC**
  Enable/Disable Rootport extensions for Downstream Port Containment.
- **URR**
  PCI Express Unsupported Request Reporting Enable/Disable.
- **FER**
  PCI Express Device Fatal Error Reporting Enable/Disable.
- **NFER**
  PCI Express Device Non-Fatal Error Reporting Enable/Disable.
- **CER**
  PCI Express Device Correctable Error Reporting Enable/Disable.
- **SEFE**
  Root PCI Express System Error on Fatal Error Enable/Disable.
- **SENFE**
  Root PCI Express System Error on Non-Fatal Error Enable/Disable.
- **SECE**
  Root PCI Express System Error on Correctable Error Enable/Disable.
- **PME SCI**
  PCI Express PME SCI Enable/Disable.
- **Hot Plug**
  PCI Express Hot Plug Enable/Disable.
- **Advanced Error Reporting**
  Advanced Error Reporting Enable/Disable.
- **PCIe Speed**
  Configure PCIe Speed.
- **Transmitter Half Swing**
  Transmitter Half Swing Enable/Disable.
- **LTR**
  SA PCIE Latency Reporting Enable/Disable.
- **Snoop Latency Override**
  Snoop Latency Override for SA PCIE.
- **Non Snoop Latency Override**
  Non Snoop Latency Override for SA PCIE.
- **LTR Lock**
  PCIE LTR Configuration Lock.
- **Peer Memory Write Enable**
  Peer Memory Write Enable/Disable.

M.2 E-Key

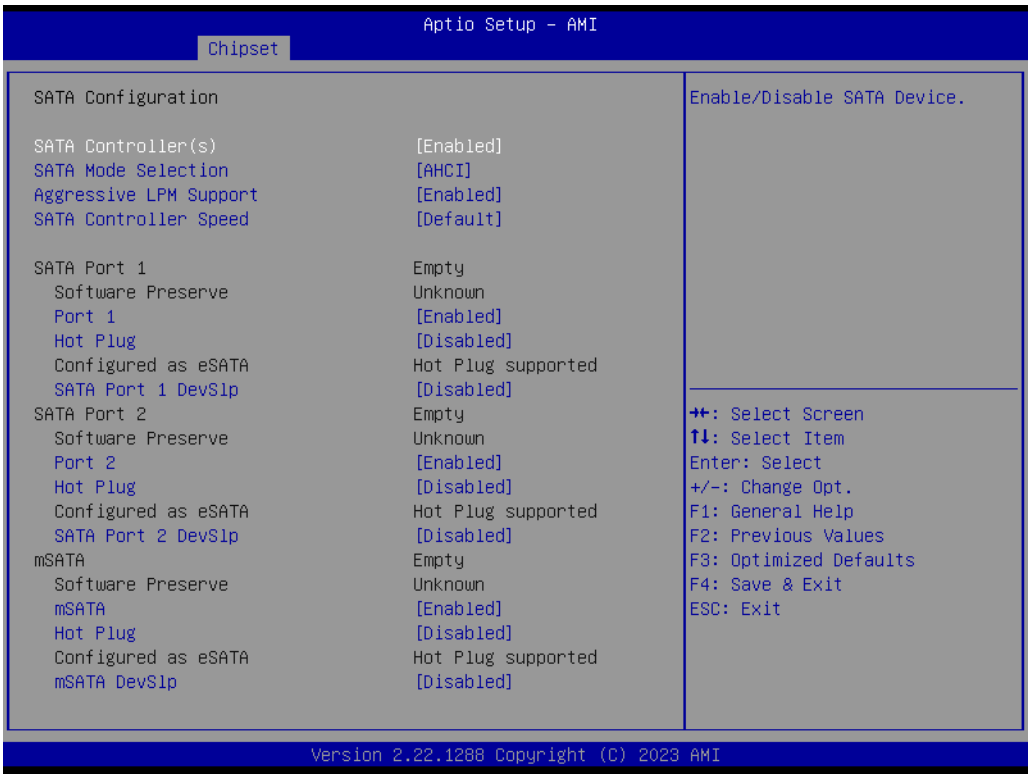
```
Aptio Setup - AMI
Chipset

PCI Express Configuration                    PCI Express Root Port Settings.

DMI Link ASPM Control          [L1]
PCIe function swap             [Enabled]
▶ PCIe EQ settings

▶ M.2 B-Key
▶ M.2 E-Key

                                             →←: Select Screen
                                             ↑↓: Select Item
                                             Enter: Select
                                             +/-: Change Opt.
                                             F1: General Help
                                             F2: Previous Values
                                             F3: Optimized Defaults
                                             F4: Save & Exit
                                             ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

```
Aptio Setup - AMI
Chipset

M.2 E-Key                          [Enabled]      Control the PCI Express Root
Connection Type                    [Slot]         Port.
ASPM                               [Disabled]
L1 Substates                       [Disabled]
L1 Low                             [Enabled]
ACS                                [Enabled]
PTM                                [Enabled]
DPC                                [Disabled]
EDPC                               [Enabled]
  URR                              [Disabled]
  FER                              [Disabled]
  NFER                             [Disabled]
  CER                              [Disabled]
  SEFE                             [Disabled]     →←: Select Screen
  SENFE                            [Disabled]     ↑↓: Select Item
  SECE                             [Disabled]     Enter: Select
  PME SCI                          [Enabled]      +/-: Change Opt.
  Hot Plug                         [Disabled]     F1: General Help
  Advanced Error Reporting         [Enabled]      F2: Previous Values
PCIe Speed                         [Auto]         F3: Optimized Defaults
Detect Non-Compliance Device       [Disabled]     F4: Save & Exit
  Transmitter Half Swing           [Disabled]     ESC: Exit
Detect Timeout                     0
Extra Bus Reserved                 0
Reserved Memory                    10

Version 2.22.1288 Copyright (C) 2023 AMI
```

```
Aptio Setup - AMI
Chipset

  URR                                [Disabled]
  FER                                [Disabled]
  NFER                               [Disabled]
  CER                                [Disabled]
  SEFE                               [Disabled]
  SENFE                              [Disabled]
  SECE                               [Disabled]
  PME SCI                            [Enabled]
  Hot Plug                           [Disabled]
  Advanced Error Reporting           [Enabled]
PCIe Speed                           [Auto]
Detect Non-Compliance Device         [Disabled]
  Transmitter Half Swing             [Disabled]
Detect Timeout                       0
Extra Bus Reserved                   0
Reserved Memory                      10
Reserved I/O                         4

PCH PCIe LTR Configuration
LTR                                  [Enabled]
  Snoop Latency Override             [Auto]
  Non Snoop Latency Override         [Auto]

LTR Lock                             [Disabled]
Peer Memory Write Enable             [Disabled]

Peer Memory Write
Enable/Disable

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

SATA Configuration

```
Aptio Setup - AMI
Chipset

PCH-IO Configuration

▶ PCI Express Configuration
▶ SATA Configuration
▶ USB Configuration
▶ Security Configuration
▶ HD Audio Configuration
▶ FIVR Configuration

LAN1 Controller                      [Enabled]
  LAN1 PXE OpROM                     [Disabled]
  Wake on LAN Enable                 [Disabled]
LAN2 Controller                      [Enabled]
  LAN2 PXE OpROM                     [Disabled]
LAN3 Controller                      [Enabled]
  LAN3 PXE OpROM                     [Disabled]
LAN4 Controller                      [Enabled]
  LAN4 PXE OpROM                     [Disabled]

PCIE Wake                            [Disabled]
Restore AC Power Loss                [Power Off]
PCIE Device Initial Delay            0
Legacy IO Low Latency                [Disabled]

SATA Device Options Settings

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```



- **SATA Controller(s)**
  Enable/Disable SATA Device.
- **SATA Mode Selection**
  Determines how SATA controller(s) operate.
- **Aggressive LPM Support**
  Enable PCH to aggressively enter link power state.
- **SATA Controller Speed**
  Indicates the maximum speed the SATA controller can support.
- **Port 1~4/mSATA**
  Enable or Disable SATA/mSATA Port
- **Hot Plug**
  SATA Hot Plug Enable/Disable.
- **SATA Port 1 DevSlp**
  Enable/Disable SATA Port 1 DevSlp. For DevSlp to work, both hard drive and SATA port need to support DevSlp function, otherwise an unexpected behavior might happen. Please check the board design before enabling it.

USB Configuration

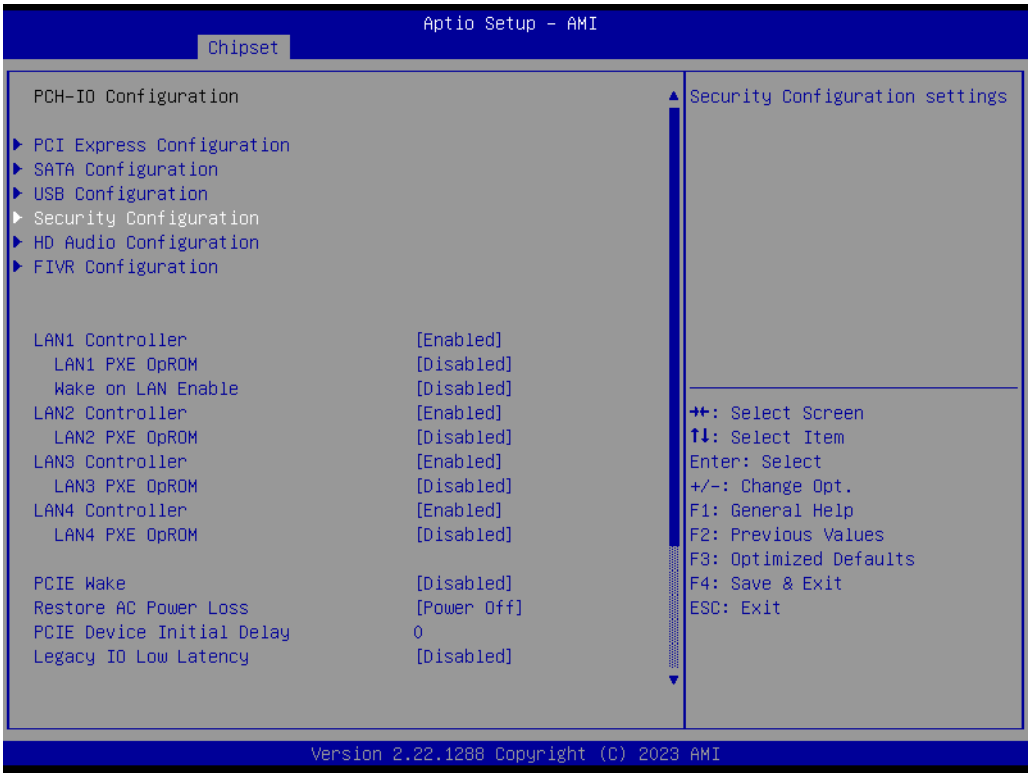
```
Aptio Setup - AMI
Chipset

PCH-IO Configuration                                  USB Configuration settings

▶ PCI Express Configuration
▶ SATA Configuration
▶ USB Configuration
▶ Security Configuration
▶ HD Audio Configuration
▶ FIVR Configuration

LAN1 Controller                    [Enabled]
  LAN1 PXE OpROM                   [Disabled]
  Wake on LAN Enable               [Disabled]
LAN2 Controller                    [Enabled]
  LAN2 PXE OpROM                   [Disabled]
LAN3 Controller                    [Enabled]
  LAN3 PXE OpROM                   [Disabled]
LAN4 Controller                    [Enabled]
  LAN4 PXE OpROM                   [Disabled]

PCIE Wake                          [Disabled]
Restore AC Power Loss              [Power Off]
PCIE Device Initial Delay          0
Legacy IO Low Latency              [Disabled]

                                   →←: Select Screen
                                   ↑↓: Select Item
                                   Enter: Select
                                   +/-: Change Opt.
                                   F1: General Help
                                   F2: Previous Values
                                   F3: Optimized Defaults
                                   F4: Save & Exit
                                   ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

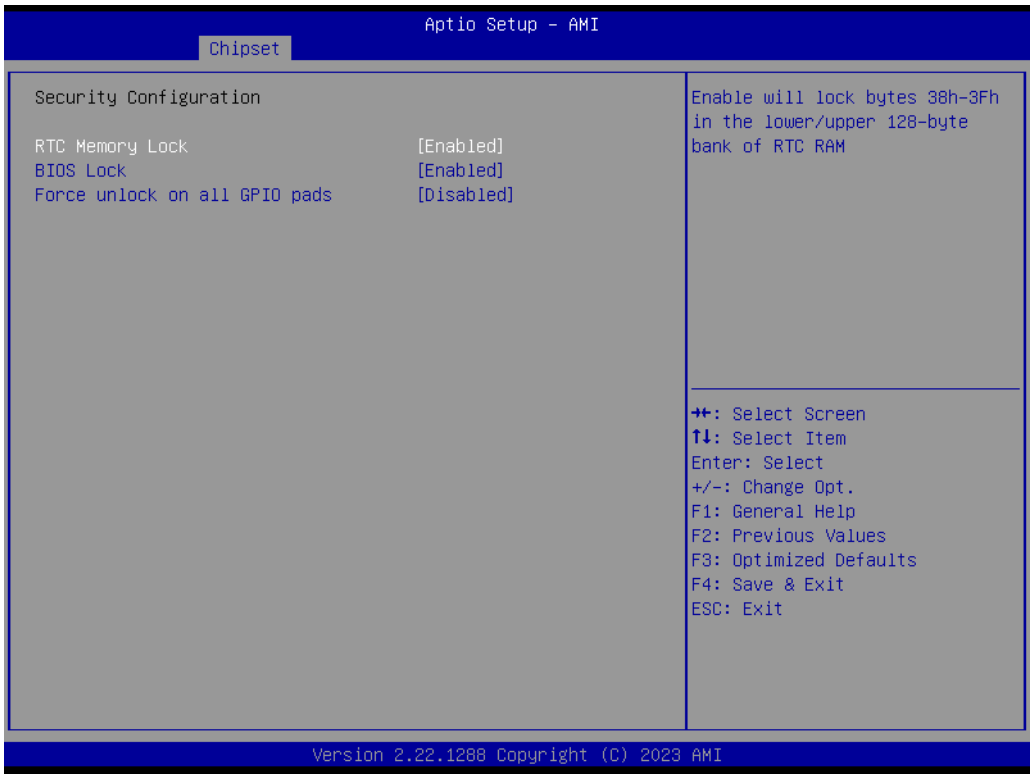
```
Aptio Setup - AMI
Chipset

USB Configuration                                     Enable/Disable xDCI (USB OTG
                                                      Device).
xDCI Support                       [Disabled]

USB PDO Programming                [Enabled]
USB Overcurrent                    [Enabled]
USB Overcurrent Lock               [Enabled]
USB Audio Offload                  [Enabled]
Enable HSII on xHCI                [Enabled]

USB3.1 Portx Speed Selection       0
USB Port Disable Override          [Disabled]

                                   →←: Select Screen
                                   ↑↓: Select Item
                                   Enter: Select
                                   +/-: Change Opt.
                                   F1: General Help
                                   F2: Previous Values
                                   F3: Optimized Defaults
                                   F4: Save & Exit
                                   ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

– **xDCI Support**
  Enable/Disable xDCI (USB OTG Device).
– **USB PD0 Programming**
  Select 'Enabled' if the Port Disable Override functionality is used.

– **USB Overcurrent**
  Select 'Disabled' for pin-based debug. If pin-based debug is enabled but USB overcurrent is not disabled, USB DbC will not work.
– **USB Overcurrent Lock**
  Select 'Enabled' if Overcurrent functionality is used. Enabling this will make xHCI controller consume the Overcurrent mapping data.
– **USB Audio Offload**
  Enable/Disable USB Audio Offload functionality.
– **Enable HSII on xHCI**
  Enable/Disable HSII feature. It may lead to increased power consumption.
– **USB3.1 Speed Selection**
  USB3.1 Speed selection; Gen1 or Gen2.
– **USB Port Disable Override**
  Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.

Security Configuration





- **RTC Memory Lock**
  Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM.
- **BIOS Lock**
  Enable/Disable the PCH BIOS Lock Enable feature. It is required to be enabled to ensure SMM protection of flash.
- **Force unlock on all GPIO pads**
  If Enabled, the BIOS will force all GPIO pads to be in the unlocked state.

HD Audio Configuration

```
Aptio Setup - AMI
Chipset

PCH-IO Configuration                                  HD Audio Subsystem
                                                      Configuration Settings
▶ PCI Express Configuration
▶ SATA Configuration
▶ USB Configuration
▶ Security Configuration
▶ HD Audio Configuration
▶ FIVR Configuration

LAN1 Controller                    [Enabled]
  LAN1 PXE OpROM                   [Disabled]
  Wake on LAN Enable               [Disabled]
LAN2 Controller                    [Enabled]
  LAN2 PXE OpROM                   [Disabled]
LAN3 Controller                    [Enabled]
  LAN3 PXE OpROM                   [Disabled]
LAN4 Controller                    [Enabled]
  LAN4 PXE OpROM                   [Disabled]

PCIE Wake                          [Disabled]
Restore AC Power Loss              [Power Off]
PCIE Device Initial Delay          0
Legacy IO Low Latency              [Disabled]

                                                      →←: Select Screen
                                                      ↑↓: Select Item
                                                      Enter: Select
                                                      +/-: Change Opt.
                                                      F1: General Help
                                                      F2: Previous Values
                                                      F3: Optimized Defaults
                                                      F4: Save & Exit
                                                      ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

```
Aptio Setup - AMI
Chipset

HD Audio Subsystem Configuration Settings             Control Detection of the
                                                      HD-Audio device.
HD Audio                           [Enabled]          Disabled = HDA will be
HDA Codec ALC245 Configuration     [No Dmic to codec] unconditionally disabled
                                                      Enabled = HDA will be
                                                      unconditionally enabled.

                                                      →←: Select Screen
                                                      ↑↓: Select Item
                                                      Enter: Select
                                                      +/-: Change Opt.
                                                      F1: General Help
                                                      F2: Previous Values
                                                      F3: Optimized Defaults
                                                      F4: Save & Exit
                                                      ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

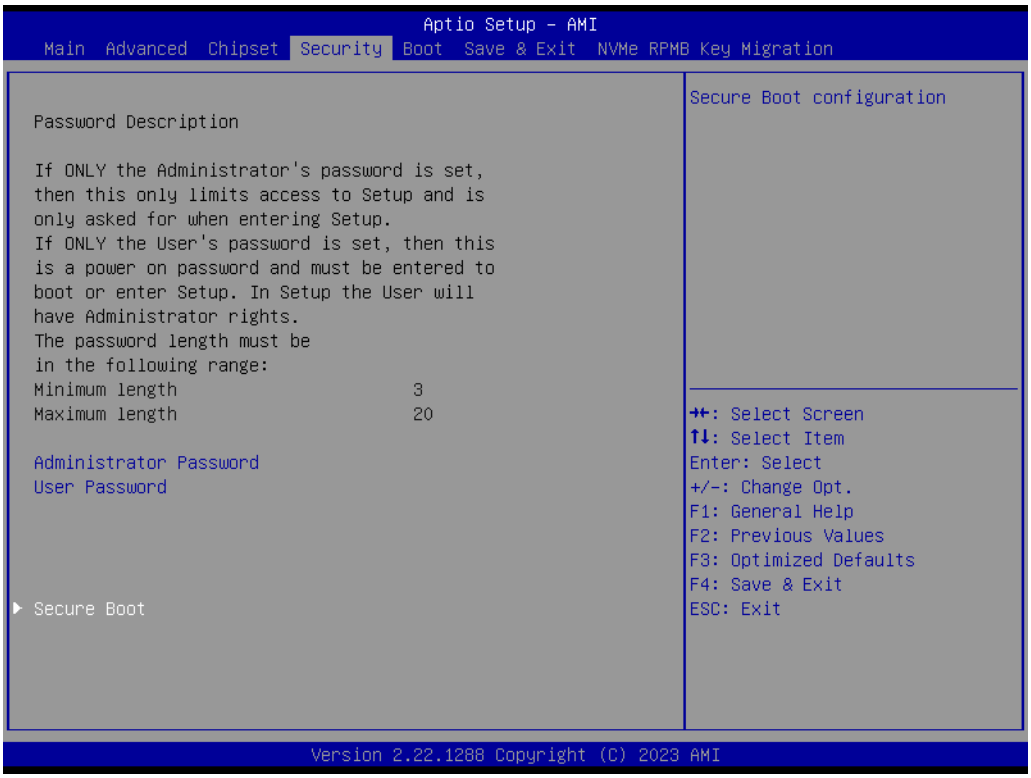
– **HD Audio**
  Control Detection of the HD-Audio device.

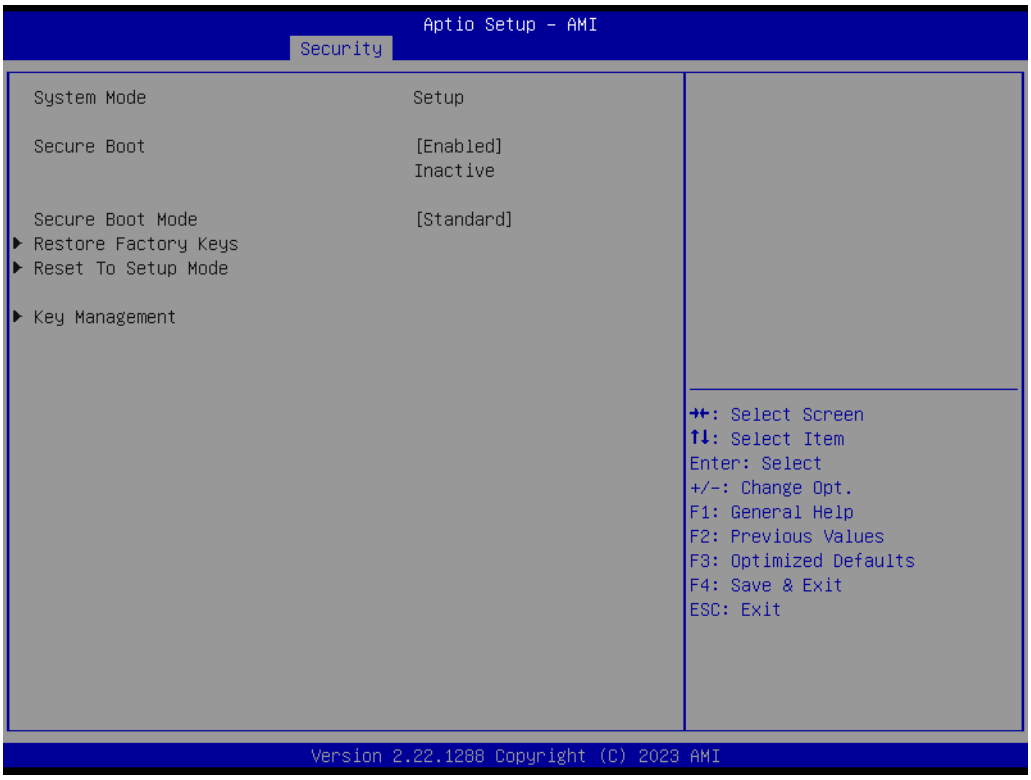
```
Aptio Setup - AMI
Chipset

PCH-IO Configuration

▶ PCI Express Configuration
▶ SATA Configuration
▶ USB Configuration
▶ Security Configuration
▶ HD Audio Configuration
▶ FIVR Configuration

LAN1 Controller                [Enabled]
  LAN1 PXE OpROM               [Disabled]
  Wake on LAN Enable           [Disabled]
LAN2 Controller                [Enabled]
  LAN2 PXE OpROM               [Disabled]
LAN3 Controller                [Enabled]
  LAN3 PXE OpROM               [Disabled]
LAN4 Controller                [Enabled]
  LAN4 PXE OpROM               [Disabled]

PCIE Wake                      [Disabled]
Restore AC Power Loss          [Power Off]
PCIE Device Initial Delay      0
Legacy IO Low Latency          [Disabled]

Menu for changing FIVR
configuration parameters

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

3.2.4 Security

```
Aptio Setup - AMI
Main  Advanced  Chipset  Security  Boot  Save & Exit  NVMe RPMB Key Migration

Password Description

If ONLY the Administrator's password is set,
then this only limits access to Setup and is
only asked for when entering Setup.
If ONLY the User's password is set, then this
is a power on password and must be entered to
boot or enter Setup. In Setup the User will
have Administrator rights.
The password length must be
in the following range:
Minimum length                 3
Maximum length                 20

Administrator Password
User Password

▶ Secure Boot

Set Administrator Password

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.22.1288 Copyright (C) 2023 AMI
```

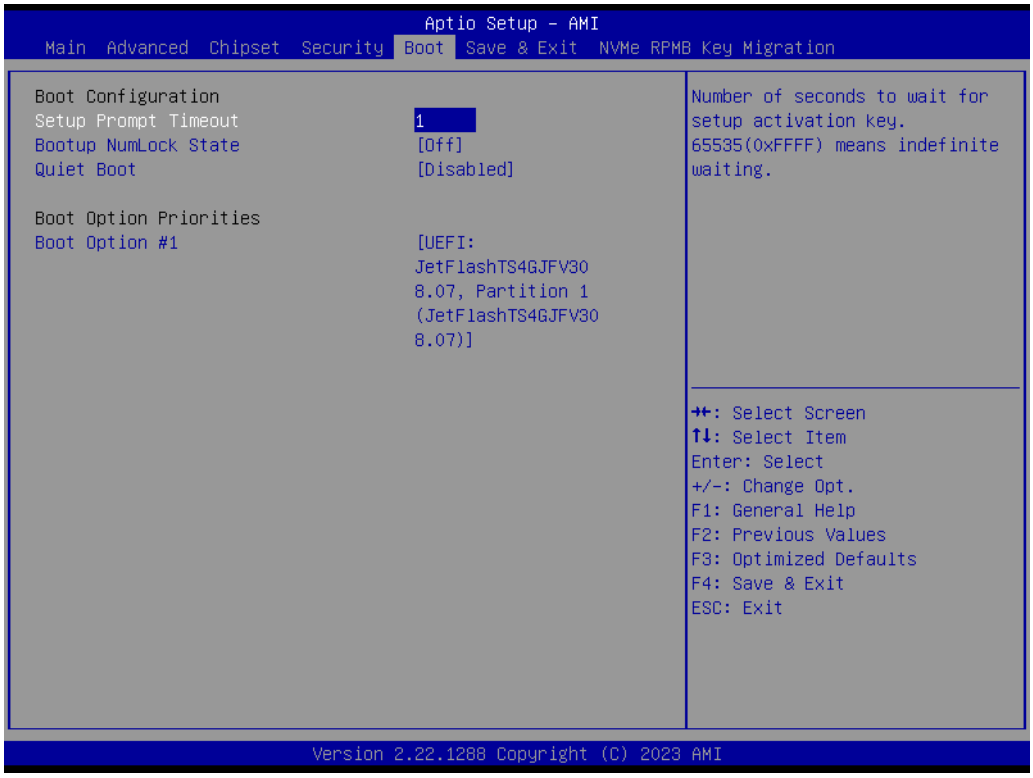
- **Administrator Password**
  Set Administrator Password.
- **User Password**
  Set User Password.





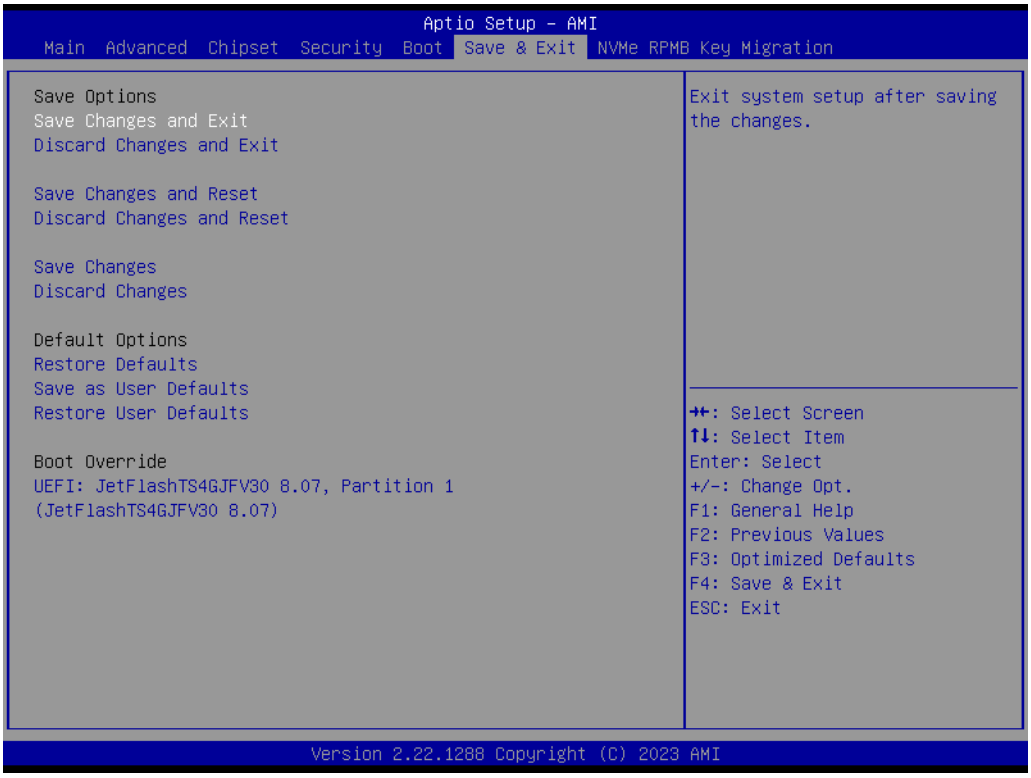
- **Secure Boot**
  The Secure Boot feature is Active if Secure Boot is Enabled, Platform Key (PK) is enrolled, and the System is in User mode. The mode change requires a platform reset.
- **Secure Boot Mode**
  Secure Boot mode options: Standard or Custom.

3.2.5 Boot



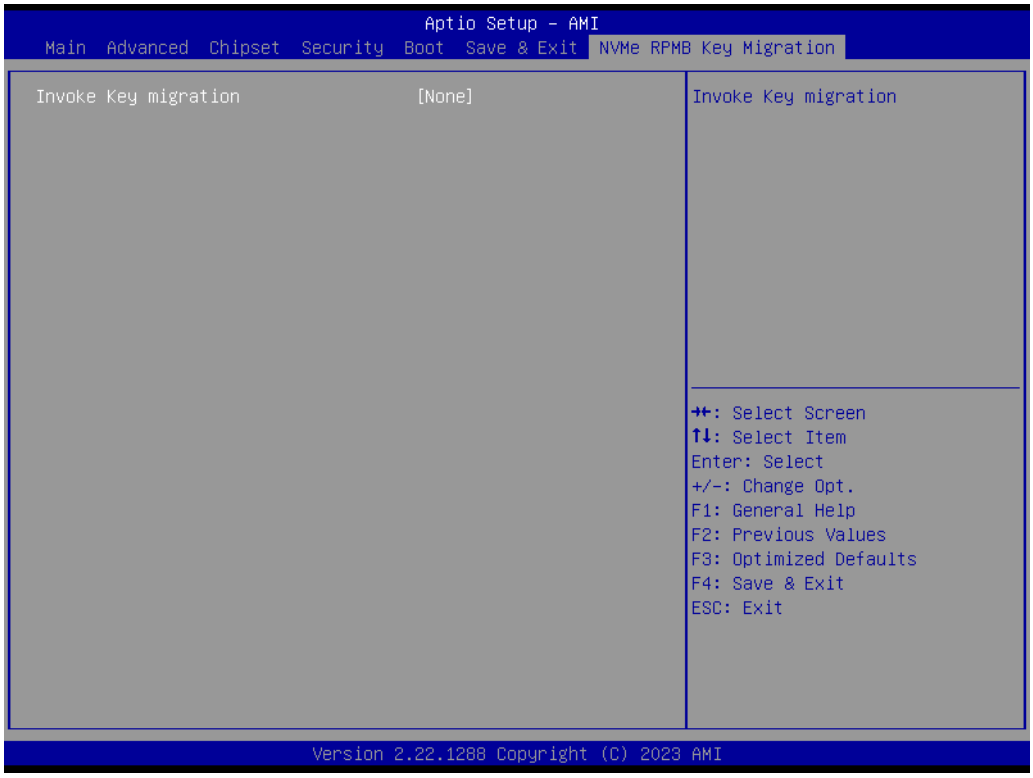
- **Setup Prompt Timeout**
  Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.
- **Bootup NumLock State**
  Select the keyboard NumLock state.
- **Quiet Boot**
  Enables or disables the Quiet Boot option.

3.2.6 Save & Exit



- **Save Changes and Exit**
  Exit system setup after saving the changes.
- **Discard Changes and Exit**
  Exit system setup without saving any changes.
- **Save Changes and Reset**
  Reset the system after saving the changes.
- **Discard Changes and Reset**
  Reset system setup without saving any changes.
- **Save Changes**
  Save Changes done so far to any of the setup options.
- **Discard Changes -> Discard Changes done so far to any of the setup options**
- **Restore Defaults**
  Restore/Load Default values for all the setup options.
- **Save as User Defaults**
  Save the changes done so far as User Defaults.
- **Restore User Defaults**
  Restore the User Defaults to all the setup options.

3.2.7 NVMe RPMB Key Migration



Provide NVMe Replay Protected Memory Block key migration function.

ADVANTECH

Enabling an Intelligent Planet

www.advantech.com

Please verify specifications before quoting. This guide is intended for reference purposes only.
All product specifications are subject to change without notice.
No part of this publication may be reproduced in any form or by any means, such as electronically, by photocopying, recording, or otherwise, without prior written permission from the publisher.
All brand and product names are trademarks or registered trademarks of their respective companies.
© Advantech Co., Ltd. 2026